Securitatea şi protecţia datelor personale în cadrul campaniilor digitale din România

Autori: Constantin Marius
Cheleș Adriana
Facultatea de Economie Agroalimentară şi a Mediului
Academia de Studii Economice din Bucureşti

Rezumat: *Scurgerea de date personale Facebook - Cambridge Analytica din anul 2016 a fost, probabil, unul dintre factorii principali care au determinat aplicarea cât mai rapidă a unui set de reglementări în spaţiul european privind protecţia datelor cu caracter personal. Astfel, în România anului 2018, mediul de afaceri este supus aplicării şi respectării Regulamentului General privind Protecția Datelor Personale (GDPR – General Data Protection Regulation). Intrat în vigoare la data de 25 mai 2018 în blocul comunitar, implicaţiile sociale şi economice ale implementării Regulamentului sunt complexe şi din acest motiv, lucrarea de faţă îşi propune evaluarea stării securităţii şi protecţiei datelor cu caracter personal furnizate în cadrul campaniilor digitale din România. Cercetarea a constat în aprecierea măsurii în care companiile analizate respectă Regulamentul General privind Protecția Datelor Personale cu ajutorul unor criterii bine stabilite ce se referă la mai multe aspecte precum: oferirea de informații referitoare la modul în care datele personale sunt prelucrate și transmisibile, oferirea posibilității de contact via e-mail/telefon, deschiderea către ștergerea sau actualizarea datelor personale din baza de date a companiei. Rezultatele cercetării ilustrează fidel gradul de siguranţă şi securitate al datelor personale furnizate companiilor în mediul digital în România. Aşadar, într-o societate profund digitalizată, este important să acceptăm faptul că datele personale sunt supuse permanent diverselor riscuri: scurgeri de date, furturi, vânzări ilegale. Este accesul la tehnologie o poartă utilizatorilor către mai multe avantaje decât dezavantaje? Concluziile lucrării oferă o viziune de ansamblu asupra tuturor acestor aspecte şi propune o serie de recomandări pentru utilizatorii care furnizează date cu caracter personal în spaţiul digital.*

Cuvinte cheie: GDPR, date personale, marketing online, securitate digitală

Abstract: *The leakage of personal data Facebook - Cambridge Analytica in 2016 was probably one of the main factors that determined the fastest implementation of a set of regulations in the European area in order to insure the protection of personal data. Thus, in 2018 in Romania, the business environment is subject to the application and compliance with the General Regulation on the Protection of Personal Data (GDPR - General Data Protection Regulation). Entered into force on May 25, 2018 in the community block, the social and economic implications of implementing the Regulation are complex and for this reason, the present paper aims to evaluate the state of security and protection of personal data provided within the digital campaigns in Romania. The research consisted in assessing the extent to which the analyzed companies comply with the General Regulation on the Protection of Personal Data with the help of well-established criteria that refer to several aspects such as: providing information on how personal data are processed and transmitted, offering the possibility of contact via email / phone, opening to delete or update personal data from the company database. The research results faithfully illustrate the degree of security and security of personal data provided to companies in the digital environment in Romania. Therefore, in a deeply digitalized society, it is important to accept that personal data is permanently subject to various risks: data leakage, theft, illegal sales. Is access to technology giving users more advantages than disadvantages? The conclusions of the paper provide an overview of all these issues and propose a series of recommendations for users who provide personal data in the digital space.*

Keywords: GDPR, date personale, marketing online, securitate digitală

Clasificare JEL: M380
Clasificare REL: 10Z

1. Introducere

Mediul de afaceri impune schimbări care sunt menite, involuntar, să determine performanţă, în condițiile în care concurenţa reprezintă elementul care influenţează agenţii economici să fie competitivi în domeniul acestora de activitate. Impactul pe care accesul la tehnologia informaţiei l-a avut şi continuă să îl aibă asupra companiilor în această era digitală

este unul profund, cu o mulţime de ramificaţii şi implicaţii de ordin tehnic, economico-social, etic şi moral etc. (Klapdor, 2013).

Companiile revizuiesc şi perfecţionează propriile campanii de promovare şi publicitate. Astfel, cele din urmă sunt adaptabile şi pot să fie optimizate, astfel încât să se adreseze cât mai bine publicului ţintă, din ce în ce mai digitalizat, mai ales în mediul urban. Conform Statista, în anul 2018 există 2,53 miliarde de utilizatori de telefoane inteligente la nivel global, cu acces la internet, ceea ce reprezintă aproximativ 34% din întreaga populație a lumii. Fiecare dintre aceştia reprezintă parte a unui public ţintă care participă la cel puţin o campanie digitală.

Prin intermediul campaniilor digitale sau al altor instrumente digitale de colectare a datelor cu caracter personal, companiile formează baze de date mai mult sau mai puțin securizate, pe care le utilizează în cadrul strategiilor de marketing, scopurile celor din urmă fiind multiple: fidelizarea și retenţia clienților, creşterea rapidă a vânzărilor, creşterea vizibilităţii companiei etc (Katz & Rice, 2002).

Astfel, într-un spaţiu digital marcat de atât de multe avantaje precum comunicarea rapidă şi eficientă, achiziţii online, acces la procese educaţionale, este important ca strategiile și politicile de stocare și protecţie a datelor cu caracter personal să fie luate în considerare serios și aplicate corect și eficient.

Un eveniment important care a dovedit importanța securității datelor personale în spațiul digital este scurgerea acestor tip de date de către Facebook, Inc. către Cambridge Analytica Ltd. în timpul campaniilor electorale din Statele Unite ale Americii din anul 2016. Expunerea datelor personale a peste 50 de milioane de utilizatori Facebook (Rosenberg et al., 2018) a amplificat necesitatea implementării, la nivelul blocului comunitar european, a Regulamentului General privind Protecția Datelor Personale (GDPR – *General Data Protection Regulation*) – legea nr. 679/2016. Data de 25 mai 2018 a marcat ziua în care Regulamentul trebuia să fie aplicat și în cazul companiilor, instituțiilor sau altor agenți care operează cu date personale în mediul virtual din România (GDPR).

2. Metodologia cercetării

Motivația elaborării lucrării este constituită dintr-un cumul de factori cu caracter juridic, tehnic, economic, social şi etic. Din punct de vedere juridic, respectarea Regulamentului implementat în spațiul european prezintă interes pentru utilizatorii paginilor si platformelor digitale, pentru că cele din urmă trebuie să respecte și să asigure integritatea datelor cu caracter personal. Astfel, se justifică necesitatea verificării legislative a securității datelor personale în mediul virtual. Abordând aceeași tematică din perspectivă tehnică, motivația provine din nevoia de a analiza și testa tehnic sistemele informatice care stochează datele personale, astfel încât, să se confirme sau nu securitatea tehnică a acestora. De asemenea, din punct de vedere economic, implementarea GDPR presupune costuri pentru agenții economici – fie cu salariile (în cazul angajaților), fie cu serviciile prestate de către contractori. Totodată, se poate observa și motivația cu caracter social: există implicații ale GDPR în piața muncii și în ceea ce vizează respectarea valorilor morale. Pe lângă cele menționate anterior, motivația elaborării lucrării mai este determinată de factori economico-sociali precum fenomenul de vânzarea-cumpărare, în medii virtuale interzise, a datelor personale furate (Linnhoff-Popien et al., 2017). Astfel, responsabilitatea protejării datelor personale se stabilește nu numai prin intermediul regulamentului, ci și prin legi sau coduri de etică. Cu toate acestea, putem afirma că regulile pe care le stabilesc comisiile de etică, în general, sunt mult mai stricte decât cele pe care le enunță Regulamentul. Spre exemplu, etica în sănătate este abordată în Codul de deontologie medicală al Colegiului Medicilor din România, prin art. 103, unde se enunță faptul că „medicul trebuie să ia toate măsurile necesare pentru protejarea intimităţii subiecţilor”. Codul de etică bancar, printre principiile și valorile sale, promovează confidențialitatea prin impunerea păstrării de către

angajați a informațiilor despre activitatea companiei sau a clienților acesteia. Confidențialitatea datelor și transparența companiilor sunt reglementate și prin intermediul legii nr. 161/19.04.2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice şi în mediul de afaceri, prevenirea şi sancționarea corupției, Cartea 1, Titlul II, Cap. I, art. 8, alin. 1, care prevede ca „principiile care stau la baza furnizării de informații şi servicii publice prin mijloace electronice sunt confidențialitatea, respectiv garantarea protejării secretului datelor cu caracter personal", dar și cu ajutorul titlului III, cap. I, art. 34, în care se subliniază „prevenirea şi combaterea criminalității informatice, asigurându-se respectarea drepturilor omului şi protecția datelor personale".

Obiectivele cercetării derivă, într-o anumită măsură, din motivația acesteia. Am propus un număr de trei obiective principale ale acestei lucrări:

- determinarea gradului de protecţie a datelor cu caracter personal furnizate de către utilizatori către companii în cadrul campaniilor digitale din România;
- verificarea integrităţii sistemelor informatice de protecţie a datelor cu caracter personal, pe care companiile din România le utilizează în cadrul campaniilor digitale;
- determinarea respectării drepturilor ce vizează propriile date personale furnizate companiilor în cadrul campaniilor digitale din România.

Urmărim îndeplinirea tuturor obiectivelor enunțate anterior prin elaborarea unei grile de evaluare care presupune acordarea unui coeficient de încredere companiilor prezente în România în ceea ce priveşte operarea cu date cu caracter personal şi protecţia acestora în cadrul campaniilor digitale. Am pornit elaborarea grilei de evaluare având în vedere obiectivele lucrării și am creat criterii de evaluare precum: oferirea de informații referitoare la modul în care datele personale sunt prelucrate și transmisibile, oferirea posibilității de contact via e-mail/telefon, deschiderea către ștergerea sau actualizarea datelor personale din baza de date a companiei etc.

Ipoteza cercetării este aceea că Regulamentului General privind Protecția Datelor Personale a fost aplicat în cadrul paginilor web și al platformelor din mediul digital, în cazul celor mai multe companii din România. Unele dintre acestea colectează date mai multe decât altele, pe care există posibilitatea să le transmită altor companii. Utilizatorilor le este menționat felul în care datele personale sunt prelucrate și pot să selecteze dacă sunt de acord sau nu ca datele acestora să fie prelucrate. Cu toate acestea, anticipăm un timp de răspuns mare în ceea ce privește furnizarea detaliilor despre felul în care datele personale sunt utilizate de către companie. De asemenea, estimăm faptul că modificarea, actualizarea sau ștergerea datelor personale durează, în medie, mai mult de 14 zile calendaristice de la data solicitării ştergerii datelor personale. Conform Regulamentului General privind Protecția Datelor Personale, termenul maxim de răspuns unei astfel de solicitări este de o lună, termen care poate să fie extins dacă agentul solicită acest lucru, cu argumente bine întemeiate.

Ulterior conceperii grilei de evaluare a protecției și securității datelor personale, am creat un profil de utilizator fictiv pentru a putea verifica și aprecia cantitativ criteriile existente în cadrul grilei de evaluare. Datele personale ale acestui cont, atașate în anexe, au fost utilizate în momentul aplicării la campaniile digitale promovate în România.

Astfel, am folosit datele personale fictive din Anexa 1 în cadrul campaniilor de promovare de la diverse companii din domeniul alimentar precum: Coca-Cola Romania, Nedelya – The Cake Company, Heidi Chocolat, Lays (PepsiCo Romania), McDonald's Romania, Ursus Breweries, Ana Pan, dar și din domeniul retail: eMAG, CEL, Cora, Carrefour, Kaufland, Metro, Mega Image. Paginile web ale campaniilor de promovare utilizate de către agenții economici menționați anterior se regăsesc în Anexa 2.

Criteriile de apreciere a încrederii protecţiei datelor personale sunt abordate în din trei perspective: o perspectivă de ansamblu (evaluare standard a protecţiei datelor personale), o altă perspectivă fundamentată pe interacţiunea cu agenţii economici (vizează evaluarea încrederii în ceea ce priveşte securitatea datelor personale în cadrul interacţiunii digitale dintre

consumator/client –companie) şi ultima perspectivă, care vizează rigoarea companiilor menţionate în Anexa 2 în ceea ce priveşte respectarea Regulamentului General privind Protecția Datelor Personale, dar şi a altor principii etice sau morale.

Criteriile standard abordate în grila de apreciere a încrederii au drept fundament legislativ art. 5 din GDPR – „Principii legate de prelucrarea datelor cu caracter personal". Complexitatea preluării datelor este astfel delimitată de faptul că datele personale cerute trebuie să fie adecvate, relevante şi limitate la ceea ce este strict necesar în raport cu scopurile în care urmează să fie prelucrate (capitolul al doilea: „Principii"). Despre modul în care operatorul oferă informații cu privire la felul de prelucrare a datelor sau oferirea posibilității de contact, regăsim în Regulament, capitolul al treilea, secțiunea 2, art. 13, faptul că operatorii sunt obligaţi să furnizeze informații cu privire la „identitatea şi datele de contact ale operatorului, datele de contact ale responsabilului cu protecţia datelor, după caz; scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării; destinatarii sau categoriile de destinatari ai datelor cu caracter personal; dacă este cazul, intenţia operatorului de a transfera date cu caracter personal către o ţară terţă sau o organizaţie". Partea a doua a grilei vizează responsabilitățile operatorului. Libertatea de control asupra datelor personale presupune și posibilitatea ștergerii sau restricționării folosirii acestora, în cazul solicitării de către persoana vizată, cadrul legal fiind asigurat prin capitolul al treilea, secțiunea 3, art. 17 care enunță „dreptul de a obține din partea operatorului ştergerea datelor cu caracter personal care o privesc, fără întârzieri nejustificate în cazul în care persoana vizată îşi retrage consimţământul pe baza căruia are loc prelucrarea". Transmiterea datelor către operatori asociați este posibilă doar prin înștiințarea persoanei avizate, conform capitolului al şaselea, secțiunea 1, art. 26, care vizează raporturile dintre operatorii asociați și persoane stabilite prin acorduri colaterale.

3. Rezultatele cercetării

Datele centralizate din tabelul 1 ilustrează realitatea din mediul virtual în ceea ce priveşte încrederea în protecţia şi securitatea datelor personale furnizate în cadrul campaniilor digitale. Astfel, constatăm faptul că toate companiile analizate colectează date cu caracter personal explicit ale participantului la campania digitală. Acest fapt scade încrederea participantului, deoarece datele sale personale sunt expuse riscurilor digitale (furturi sau scurgeri de date personale etc). Cu toate acestea, participantului îi sunt prezentate, în cazul tuturor campaniilor analizate, informaţii şi detalii referitoare la felul în care datele personale sunt prelucrate. De asemenea, acestuia îi este oferită posibilitatea de a contacta via e-mail sau formular comaniile care îi prelucrează datele cu caracter personal. Spre deosebire de cele două aspectele pozitive enunţate anterior, care întăresc încrederea utilizatorului în securitatea datelor personale transmise, nu toate campaniile digitale analizate oferă posibilitatea de contact via telefon, mobil sau fax. Companii precum Lays (PepsiCO), CocaCola, Ursus, McDonalds, Carrefour, Kaufland, Metro şi Mega Image nu oferă disponibil niciun număr de telefon la care utilizatorul ar putea recurge pentru a afla mai multe detalii despre datele sale personale.

Cercetarea a presupus, printre altele, şi interacţiunea directă cu agenţii economici menţionaţi în Anexa 2 pentru a verifica respectarea legislaţiei protecţiei datelor personale. Acestora le-a fost solicitat să furnizeze explicit detalii privind datele personale utilizate (modul de folosire şi prelucrare, alte detalii relevante) dar şi să şteargă datele personale din baza de date. Dintre cele 14 companii, trei dintre acestea au răspuns automat la solicitările via e-mail (21%), iar alte patru au răspuns prin intermediul unui angajat sau prin intermediul unui responsabil cu protecţia datelor personale (28%). De la restul de şapte companii (50% din total) nu am primit niciun răspuns în termen de 14 zile calendaristice referitor la solicitarea enunţată anterior. Acest lucru justifică încrederea scăzută a utilizatorilor în ceea ce priveşte protecţia şi securitatea propriilor date personale furnizate companiilor în mediul digital şi determină scăderea cu 335 de puncte a gradului de încredere, evaluat în tabelul 1. Deşi legislaţia este implementată în cazul

tuturor celor 14 companii analizate, timpul de răspuns şi interacţiune cu publicul este unul ridicat şi depăşeşte 14 zile calendaristice. Conform GDPR, companiile au obligaţia să răspundă solicitărilor în termen de o lună de la primirea acesteia, termen care poate să fie extins în condiţii speciale. Totuşi, considerăm că termenul stabilit prin lege este unul destul de mare şi nu oferă utilizatorilor eficienţă în ceea ce priveşte managementul timpului. Interacţiunea cu companiile care utilizează datele personale în mediul digital trebuie să fie una rapidă, eficientă şi transparentă, cu toate că acest fapt poate să impună costuri ridicate pentru companie (cu salariaţii sau cu achiziţia de servicii de tip customer support de la alte companii). Totodată, gradul de încredere în protecţia datelor personale este scăzut, deoarece datele personale furnizate companiilor în mediul digital sunt transmisibile altor companii, grupuri sau agenţi, fapt ce este confirmat în politica de confidenţialitate a 78% dintre companiile analizate sau în momentul solicitării via e-mail a informaţiilor suplimentare care vizează politica de circulaţie a datelor personale.

Tabelul 1

Grila de evaluare a încrederii acordate în privinţa protecţiei datelor personale în cadrul campaniilor de promovare digitale din România în domeniul alimentar şi retail

CRITERII DE APRECIERE A ÎNCREDERII PROTECŢIEI DATELOR CU CARACTER PERSONAL	BAREMUL DE NOTARE	DOMENIUL ALIMENTAR							DOMENIUL RETAIL						
		Lays	Heidi	Coca Cola	Ursus	Nedelya	Mc Donalds	Ana Pan	eMAG	CEL	Cora	Carre four	Kaufland	Metro	Mega Image
		GRAD DE ÎNCREDERE													
1. CRITERII STANDARD DE APRECIERE A ÎNCREDERII PROTECŢIEI DATELOR CU CARACTER PERSONAL															
Colectează date cu caracter personal explicit despre participant	DA: 0 puncte NU: 5 puncte	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Oferă informaţii despre felul în care sunt prelucrate datele cu caracter personal ale participanţilor	DA: 10 puncte NU: -10 puncte	10	10	10	10	10	10	10	10	10	10	10	10	10	10
Oferă posibilitatea de contact via e-mail sau form	DA: 10 puncte NU: -10 puncte	10	10	10	10	10	10	10	10	10	10	10	10	10	10
Oferă posibilitatea de contact via telefon, mobil sau fax	DA: 5 puncte NU: -5 puncte	-5	5	-5	-5	5	-5	5	5	5	5	-5	-5	-5	-5
2. CRITERII DE APRECIERE A ÎNCREDERII PROTECŢIEI DATELOR PERSONALE, BAZATE PE INTERACŢIUNEA CU AGENŢII ECONOMICI															
Răspund la metodele de contact oferite, în termen de 14 zile calendaristice	DA: 15 puncte AUTOMAT: 0 puncte NU: -15 puncte	-15	0	0	-15	15	15	15	0	-15	15	-15	-15	-15	-15
Furnizează explicit, via e-mail, detalii privind datele participanţilor înregistraţi (modul de folosire, prelucrate etc)	DA: 15 puncte PARŢIAL: 5 puncte NU: -15 puncte	-15	-15	-15	-15	5	15	15	-15	-15	-15	-15	-15	-15	-15
Actualizează sau şterg datele personale, conform cerinţelor participanţilor	DA: 20 puncte NU: -20 puncte	-20	-20	-20	-20	20	20	20	-20	-20	-20	-20	-20	-20	-20
Datele personale furnizate companiei sunt transmisibile altor companii/grupuri	DA: -10 puncte NU: 10 puncte	-10	10	-10	-10	10	-10	10	-10	-10	-10	-10	-10	-10	-10
3. CRITERII DE APRECIERE A ÎNCREDERII PROTECŢIEI DATELOR PERSONALE, BAZATE STRICT PE RIGOAREA RESPECTĂRII REGLEMENTĂRILOR GDPR															
CII, Art. 8: *Copiii au nevoie de o protecţie specifică a datelor personale*	ACORDĂ: 5 puncte NU ACORDĂ: -5 puncte	5	5	-5	5	-5	5	-5	-5	-5	-5	-5	-5	-5	5
S2, Art. 32: *Operatorii asigură securitatea datelor personale prin testarea şi evaluarea periodică a eficacităţii măsurilor tehnice*	DA: 5 puncte NU MENŢIONEAZĂ: - 5 puncte	-5	-5	5	-5	5	5	-5	5	5	5	5	-5	5	5
TOTAL	100 puncte	-45	0	-30	-45	75	65	75	-20	-35	-5	-45	-55	-45	-35
MEDIE GENERALĂ PER DOMENIU		13,57							-34,29						
MEDIE GENERALĂ		-10,36													

Sursa: Conceptualizare proprie, pe baza datelor prelucrate

Din punct de vedere pur legislativ, conform Regulamentului General privind Protecţia Datelor Personale: „*Copiii au nevoie de protecţie specifică a datelor cu caracter personal, întrucât pot fi mai puţin conştienţi de riscurile, consecinţele şi drepturile lor în ceea ce priveşte prelucrarea datelor cu caracter personal.*” Acest criteriu este integrat în grila de apreciere a încrederii protecţiei datelor personale şi realitatea din mediul digital nu este una favorabilă companiilor analizate, deoarece doar 35% dintre acestea au elaborat reglementări specifice destinate datelor personale ale copiilor. De asemenea, secţiunea 2, art. 32 din Regulamentul General privind Protecţia Datelor Personale prevede faptul că operatorul, dar şi persoana împuternicită de acesta, implementează măsuri tehnice în vederea asigurării unui nivel de protecţie şi securitate pe măsura riscurilor, prin testarea şi evaluarea periodică a eficienţei măsurilor tehnice. Puţin peste jumătate din operatorii analizaţi (64%) menţionează existenţa şi

implementarea unei astfel de reglementări tehnice în politica de confidenţialitate a datelor personale sau în alte secţiuni cu caracter tehnic existente în cadrul paginilor web sau în cadrul platformei utilizate de colectare şi prelucrare a datelor personale.

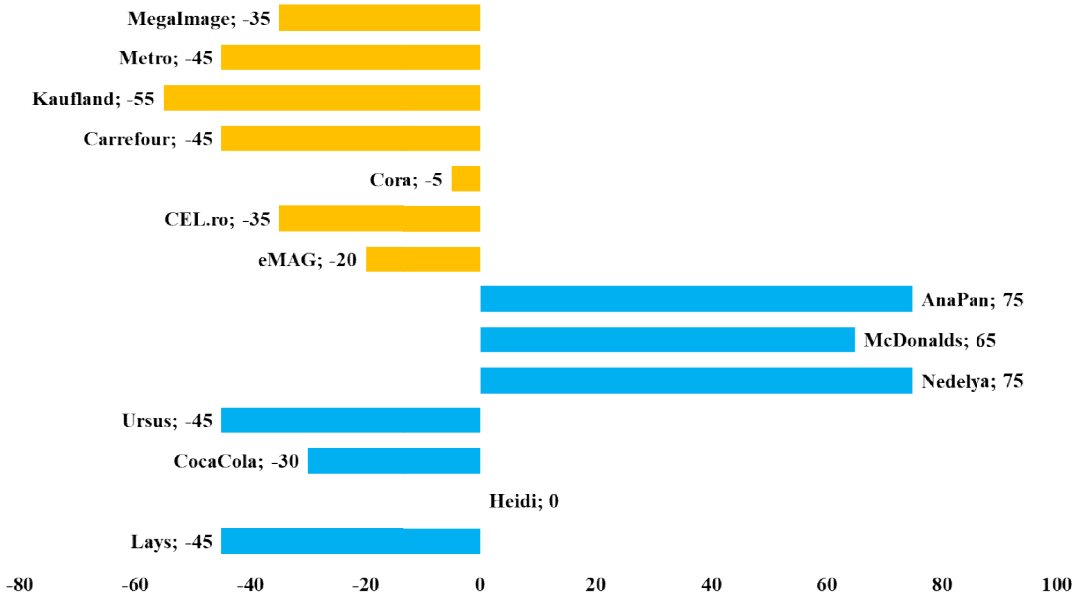

Fig. 1. Rezultatele individuale ale evaluării încrederii acordate în privinţa protecţiei datelor personale în cadrul campaniilor de promovare digitale din România în domeniul alimentar şi retail
Sursa: Conceptualizare proprie, pe baza datelor prelucrate

Comparăm rezultatele obţinute de către domeniul alimentar cu cele ale domeniului retail şi observăm faptul că domeniul alimentar acordă mai multă atenţie respectării şi aplicării Regulamentului și protejării datelor persoanelor, în general (media acestui domeniu este cu 47,8 mai mare decât cea a domeniului retail). Conform figurii 1, se observă faptul că AnaPan, McDonalds şi Nedelya sunt cele trei companii care au contribuit decisiv în obţinerea unui grad ridicat de încredere în ceea ce priveşte protecţia şi securitatea datelor personale în mediul digital: 75, 65, respectiv 75 de puncte, obţinând astfel cele mai mari punctaje dintre toate companiile analizate. Acest fapt este cauzat de faptul că cele trei companii amintite anterior au fost singurele care au răspuns afirmativ solicitării ştergerii datelor personale din baza de date în termen de 14 zile calendaristice, deşi termenul legal este de o lună. Pe de o parte, acest fapt dovedeşte interesul pentru respectarea şi aplicarea Regulamentului General privind Protecția Datelor Personale, iar pe de altă parte, acest fapt poate să dovedească şi devotamentul pe care AnaPan, McDonalds şi Nedelya îl arată pentru clienţii acestora, deoarece sunt eficienţi şi agili atunci când se confruntă cu solicitări din partea acestora. Figura 2 ilustrează distanţa considerabilă de 86,43 respectiv 134,29 de puncte faţă de punctajul maxim de 100, ceea ce ilustrează deficienţe în ceea ce priveşte percepţia utilizatorilor faţă de securitatea şi protecţia datelor personale transmise în cadrul campaniilor digitale agenţilor şi operatorilor din domeniul alimentar şi domeniul retail.

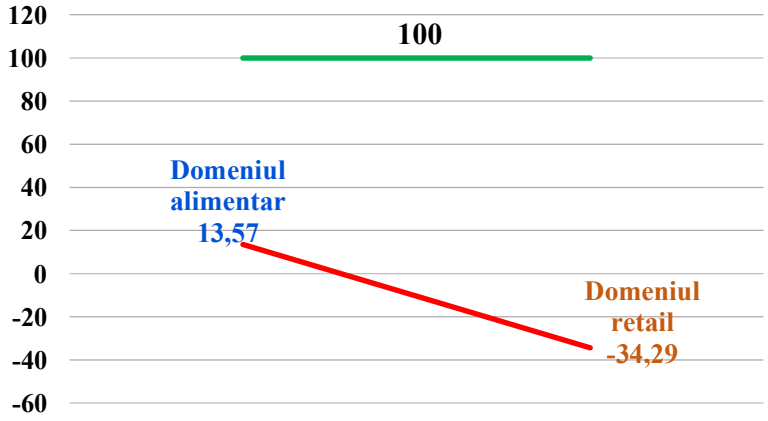

Fig. 2. Rezultatele evaluării încrederii acordate în privinţa protecţiei datelor personale în cadrul campaniilor de promovare digitale din România în domeniul alimentar şi retail

Sursa: Conceptualizare proprie, pe baza datelor prelucrate

În măsura în care companiile analizate ar dedica mai mult timp şi resurse pentru racordarea obiectivelor acestora la nevoile şi solicitările clienţilor/utilizatorilor, cu siguranţă că încrederea celor din urmă în datele personale furnizate, implicit în securitatea şi protecţia acestora, s-ar îmbunătăţii, în schimbul costurilor suplimentare pe care companiile le-ar suporta. Cercetarea indică faptul că s-au făcut demersuri în acest sens, însă doar de către un număr limitat de companii.

4. Concluziile, propunerile şi limitele cercetării

În cele din urmă, constatăm faptul că obiectivele cercetării au fost îndeplinite. Gradul de protecție a datelor personale furnizate în cadrul campaniilor digitale analizate din România a fost determinat și este unul suficient de scăzut: -10,36 (din maxim 100), conform grilei de evaluare a încrederii protecţiei datelor personale, rezultat ce se suprapune ipotezei cercetării, iar cauzele sunt multiple: timpul mare de așteptare pentru a primi un răspuns și pentru ștergerea datelor personale (mai mare decât 14 zile calendaristice), practicarea unei politici netransparente de furnizare a informațiilor privind utilizarea datelor personale și transferul acestora către alte companii sau agenți, lipsa testării regulate a sistemului informatic ce stochează datele personale (sau lipsa informării desfășurării unei astfel activități în termenii de utilizare ai platformelor sau a paginilor web) etc. De asemenea, am verificat integritatea sistemelor informatice ce stochează date personale pe care companiile le utilizează în cadrul campaniilor digitale și acestea funcționează optim: înregistrarea, ștergerea și re-înregistrarea în baza de date se poate efectua fără dificultăți, în cadrul campaniilor digitale analizate. Totodată, urmărind îndeplinirea ultimului obiectiv propus, am constatat faptul că cele mai importante drepturile ce vizează datele personale furnizate în cadrul campaniilor digitale din România sunt respectate de către operatorii analizați. Astfel, având un caracter obligatoriu, legislația din domeniu este aplicată de companiile analizate.

La nivelul companiilor analizate, am remarcat următoarele aspecte care vizează gradul de protecție a datelor personale în mediul digital din România: toate dintre acestea colectează date cu caracter personal explicit despre clienții acestora în mediul digital; toate acestea oferă informații clare și cât mai complete despre felul în care prelucrează și protejează datele personale ale utilizatorilor online; toate dintre acestea pot să fie contactate via e-mail/form în mediul digital, dar nu toate (doar 42%) pun la dispoziția utilizatorilor modalități de contact via telefon, mobil, fax; în peste 78% din cazurile analizate, timpul de răspuns la solicitări via e-mail, timpul de răspuns a depășit pragul stabilit de 14 zile calendaristice, ceea ce poate determina dubii în

rândul utilizatorului referitoare la securitatea propriilor date persoane furnizate; doar 35% dintre acestea au elaborat reglementări și politici specifice, adresate datelor personale ale copiilor; aproximativ 64% dintre acestea susțin că asigură securitatea și protecția datelor personale prin testarea și evaluarea periodică a eficienței sistemelor informatice de colectare și preluare a datelor persoanle ale utlizatorilor.

Finalitatea cercetării scoate în evidență o serie de propuneri și sugestii pentru companiile analizate, din punctul de vedere al securității datelor personale furnizate de către utilizatori. Propunem ca timpul de răspuns solicitărilor utilizatorilor ce vizează datele personale ale acestora să fie redus, să fie implementate politici de colectare și protejare a datelor personale ale copiilor, să fie integrate practici de verificare și testare regulate ale sistemelor informatice care colectează și stochează datele personale ale utilizatorilor și oferirea posibilităților de contact prin intermediul telefonului/mobilului.

Cu toate acestea, cercetarea a fost efectuată în cazul unui număr limitat de campanii digitale: 14, din doar două domenii: domeniul alimentar și domeniul retail. Aceasta poate reprezenta una dintre limitele cercetării. Aplicarea metodologiei asupra mai multor campanii digitale din România, din mai multe domenii, ar surprinde mult mai fidel starea securității și protecției datelor personale, rezultatele fiind astfel mult mai reprezentative la nivelul întregului mediu de afaceri românesc. De asemenea, în cadrul lucrării a fost abordat un număr limitat de reguli, legi și alte aspecte juridice, morale sau etice din domeniul securității și protecției datelor personale. O analiză mult mai strictă și severă ar presupune studierea mai amănunțită și detaliată a tuturor acestor aspecte în cazul fiecărei campanii digitale.

Așadar, securitatea și protecția datelor personale în mediul digital a devenit un subiect delicat și absolut necesar de abordat în cazul campaniilor de promovare online din România. Aplicarea și respectarea Regulamentului General privind Protecția Datelor Personale este o condiție esențială pentru care toți operatorii de date personale trebuie să acorde o atenție deosebită.

Bibliografie

1. Katz, J. & Rice, R. (2002). *Social Consequences of Internet Use: Access, Involvement, and Interaction, 2002*;
2. Klapador, S. (2013). *Effectiveness of online marketing campaigns: an investigation into online multichannel and search engine advertising*;
3. Rosenberg, M., Confessore, N, Cadwalladr, C. (2018). *How Trump Consultants Exploited the Facebook Data of Millions*;
4. Linnhoff-Popien, C., Schneider, R., Zaddach, M. (2017). *Digital Marketplaces Unleashed*;
* Asociaţia Română a Băncilor – *Codul de etică bancară*;
* Colegiul Medicilor din România – *Codul de deontologie medicală*;
* Official Journal of the European Union – *General Data Protection Regulation*.

ANEXA 1. Datele personale fictive folosite în cadrul cercetării

Nume şi prenume: Popescu Ion
Adresa de e-mail: popescuionn2018@gmail.com
Parola adresei de e-mail: testingGDPR123
Data naşterii: 10.10.1995
Numărul de telefon: +40 (729) 182 831
Localitate: Bucureşti

ANEXA 2. Paginile web ale campaniilor de promovare analizate în cadrul cercetării

I. DOMENIUL ALIMENTAR:
1. Lays: https://www.lays.ro/
2. Heidi Chocolat: https://www.neplictisitor.ro/
3. Coca-Cola Romania: https://www.coca-cola.ro/ro/home/
4. Ursus Breweries: https://momente.cool/
5. Nedelya – The Cake Company: https://nedelya.ro/
6. McDonald's Romania: https://mcdonalds.ro/mobile/index.php/pages/home
7. Ana Pan: https://www.anapan.ro/5-zile-de-cadouri-cu-uber.html

II. DOMENIUL RETAIL:
1. eMAG: https://www.emag.ro/campaign/reduceri-de-stoc
2. CEL: http://www.cel.ro/promotii/0i-1
3. Lidl: https://www.lidl.ro/ro/index.htm
4. Carrefour: https://carrefour.ro/promotii-carrefour
5. Kaufland: https://www.kaufland.ro/oferte/saptamana-curenta.html
6. Metro: https://www.metro.ro/ofertele-zilei/cataloagele-metro
7. Mega Image: https://www.mega-image.ro/campanii-si-promotii-in-magazine

**Pagini web accesate la data de 10 octombrie 2018.*