OBȚINEREA CONSIMȚĂMÂNTULUI PERSOANEI VIZATE ÎN TEORIE ȘI ÎN PRACTICĂ

Anita **Boros**[1)]

Rezumat: *Regulamentul privind protecția datelor cu caracter personal impune o abordare mult mai transparentă în ceea ce privește obținerea consimțământului pentru prelucrarea datelor cu caracter personal. Multe companii riscă să nu se conformeze legii dacă nu reușesc să abordeze modul în care obțin consimțământul persoanei vizate. Acest articol oferă o analiză aprofundată a noțiunii de „consimțământ" și clarifică cerințele pentru obținerea și dovedirea consimțământului valabil. Totodată, vom prezenta câteva cazuri mult întâlnite în practică, care necesită o atenție sporită din partea operatorilor de date, pentru a se asigura că utilizează consimțământul ca temei juridic pentru prelucrarea datelor în conformitate cu legile aplicabile.*

Cuvinte-cheie: *consimțământul persoanei vizate; trimitere newsletter; cookie-uri; consimțământ la loc de muncă.*

Summary: *The General Data Protection Regulation requires a much more transparent approach to gaining consent to process personal data. Many companies are running the risk of non-compliance with the law if they fail to address how data is obtained and the lack of true consent which data subjects currently give to their data being processed. In this study we will clarify the notion of consent and we will present some practical cases in which the data controllers need to pay attention to, to ensure that they use consent as a legal ground for data processing in accordance with applicable laws.*

Keywords: *consent; newsletter; cookies; employee consent.*

[1)] Anita Boros este avocat, membru în Baroul Cluj, student doctorand la Școala Doctorală din cadrul Universității Eötvös Loránd din Budapesta. Poate fi contactată la adresa de e-mail *anita.a.boros@gmail.com*.

1. Introducere

Consimțământul persoanei vizate este unul dintre cele șase temeiuri legale ale operațiunilor de prelucrare de date prevăzute în Regulamentul general privind protecția datelor cu caracter personal[2]. Deși, conform Regulamentului, nu există o ierarhie în ceea ce privește temeiurile prelucrării datelor prevăzute la art. 6 alin. (1), în practică, putem observa că operatorii de date preferă să folosească consimțământul persoanei vizate pentru asigurarea legalității de prelucrare a datelor, chiar dacă, pentru obținerea unei consimțământ valabil, este nevoie de îndeplinirea mai multor criterii. Ca să fie valabil exprimat, consimțământul trebuie să îndeplinească atât cerințele prevăzute de Regulament, cât și pe cele prevăzute de Codul civil[3].

Având în vedere provocările pe care le ridică obținerea unei consimțământ valabil conform Regulamentului, se impune o analiză complexă cu privire la bune practici în obținerea consimțământului, care, pentru persoanelor vizate, oferă controlul prelucrării datelor sale, iar, pentru operator, constituie o modalitate de autorizare a procesării acestor date.

În prezenta lucrare, vom analiza mai întâi condițiile esențiale prevăzute de Regulament pentru obținerea consimțământului valabil, după care vom prezenta câteva cazuri practice în care folosirea consimțământului pentru legitimarea prelucrărilor de date poate constitui o adevărată provocare.

2. Obținerea consimțământului în teorie

În timp ce Directiva 95/46/CE, abrogată în prezent, a definit consimțământul ca fiind „*orice manifestare de voință, liberă, specifică și informată prin care persoana vizată acceptă să fie prelucrate datele cu caracter personal care o privesc*”[4], Regulamentul definește consimțământul ca fiind „*orice manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta accepta, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate*”[5].

Așadar, putem observa că Regulamentul stabilește un standard mai ridicat în ceea ce privește condițiile consimțământului, având în vedere că, pe lângă respectarea elementelor deja existente în Directivă, conform legislației în vigoare, sunt necesare practici și mecanisme bine gândite, ceea ce dovedește obținerea consimțământului fără echivoc. Cerința caracterului neechivoc o găsim și în art. 5 alin. (1) din Legea nr. 667/2001[6], însă nici Directiva 95/46/CE, nici Legea nr. 667/2001 nu explică semnificația acestuia[7]. Dar Regulamentul aduce clarificări în acest sens. Așadar, pentru un consimțământ valid, acestea trebuie să îndeplinească cerințele enunțate în cele ce urmează.

[2] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), publicat în J. Of., seria L, nr. 119/1 din 4 mai 2016 (în continuare, „Regulament”), pp. 1-88.

[3] Art. 1.204 C.civ. prevede că: „Consimțământul părților trebuie să fie serios, liber și exprimat în cunoștință de cauză”.

[4] Art. 2 lit. (h) din Directiva 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date, abrogată în prezent.

[5] Art. 4 pct. 11 din Regulament.

[6] Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date (publicată în M. Of. nr. 790 din 12 decembrie 2001 și abrogată prin Legea nr. 129/2018, la 25 mai 2018).

[7] *S. Crețu*, Consimțământul. Reguli noi pentru un temei tradițional de prelucrare a datelor personale, în A. Săvescu (coord.), RGPD. Regulamentul general privind protecția datelor cu caracter personal. Comentarii și explicații, Ed. Hamangiu, București, 2018, p. 33.

2.1. Consimțământul să fie liber exprimat

Elementul „liber" implică posibilitatea reală și efectivă a persoanelor vizate de a accepta ca datele care le aparțin să fie prelucrate pentru scopuri clar determinate, în lipsa oricăror constrângeri. Astfel, ca regulă generală, în cazul în care persoana se simte obligată să consimtă sau există riscul că va suferi consecințe negative în cazul în care nu consimte, consimțământul nu va fi valabil[8].

În acest sens, chiar și Regulamentul reține situații exemplificative (nu limitative) în care consimțământul nu va fi liber exprimat. Art. 7 alin (4) prevede că: „*atunci când se evaluează dacă consimțământul este dat în mod liber, se ține seama cât mai mult de faptul că, printre altele, executarea unui contract, inclusiv prestarea unui serviciu, este condiționată sau nu de consimțământul cu privire la prelucrarea datelor cu caracter personal care nu este necesară pentru executarea acestui contract*".

Așa cum putem observa, trebuie să evităm situațiile în care consimțământul pentru prelucrarea datelor cu caracter personal devine o contraprestație pentru executarea obligațiilor cocontractantului. Astfel, în raporturile contractuale, întotdeauna trebuie să existe o legătură directă și obiectivă între prelucrarea de date cu caracter personal și scopul executării contractului, iar, dacă există, fundamentul prelucrării datelor îl va constitui ipoteza reglementată la art. 6 alin. (1) lit. (b) din Regulament („prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract") și nu este necesar ca operatorul să utilizeze un alt temei juridic, cum este obținerea consimțământului persoanelor vizate[9]. Constrângerea de a fi de acord cu utilizarea datelor personale în plus față de cele strict necesare limitează opțiunile persoanei vizate și împiedică manifestarea liberă a consimțământului. Având în vedere că protecția datelor are ca scop protejarea drepturilor fundamentale ale omului, un control al persoanei asupra datelor sale cu caracter personal este esențial și există o prezumție puternică potrivit căreia consimțământul privind prelucrarea datelor care nu sunt necesare, nu poate fi văzut ca o cerință obligatorie în schimbul executării contractului sau furnizării unui serviciu[10].

În al doilea rând, consimțământul nu va fi valabil obținut nici în cazul în care un serviciu implică mai multe operațiuni de prelucrare, servind mai multor scopuri, iar persoanele vizate nu au posibilitatea de a-și exprima acordul pentru fiecare operațiune în parte, ci sunt nevoite să adere necondiționat la un „pachet" de scopuri de prelucrare. În asemenea situații, este nevoie de separarea scopurilor și solicitarea unui consimțământ distinct pentru fiecare scop în parte, așa cum prevede și considerentul (32) din Regulament, care subliniază că „*consimțământul ar trebui să vizeze toate activitățile de prelucrare efectuate în același scop sau în aceleași scopuri. Dacă prelucrarea datelor se face în mai multe scopuri, consimțământul ar trebui dat pentru toate scopurile prelucrării*".

Totodată, conform considerentului (43) din Regulament, consimțământul nu va fi liber exprimat dacă există un dezechilibru evident între persoana vizată și operator. Astfel de situații putem întâlni în cazul raporturilor dintre cetățeni și autoritățile publice sau chiar în cazul raporturilor de muncă dintre angajați și angajatori, în care persoana vizată nu va avea la dispoziție o alternativă realistă la acceptarea prelucrării din

[8] Grupul de lucru „Articolul 29", Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, adoptate la 4 mai 2020, p. 8.

[9] *I.A. Micu, Y. Bețleagă*, Revizuirea Ghidului privind consimțământul – un pas în plus către implementarea GDPR, Universul Juridic, disponibil la adresa *https://www.universuljuridic.ro/revizuirea-ghidului-privind-consimtamantul-un-pas-in-plus-catre-implementarea-gdpr/*, accesată în data de 01.07.2018.

[10] Grupul de lucru „Articolul 29", Orientări asupra consimțământului în temeiul Regulamentului 2016/679, adoptate la 28 noiembrie 2017, p. 7.

partea unui astfel de operator[11]. În asemenea cazuri, trebuie să analizăm dacă, în concret, persoana vizată are posibilitatea reală de a accepta sau refuza prelucrarea propusă de operator.

Nu în ultimul rând, operatorul trebuie să demonstreze că retragerea consimțământului nu conduce la niciun cost sau pierdere pentru persoana vizată și, prin urmare, nu prezintă un dezavantaj clar pentru cei care își retrag sau refuză să ofere consimțământul, așa cum prevede considerentul (42) din Regulament: „*consimțământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată*”.

Prejudiciul, în acest sens, poate consta nu numai în pagube materiale, ci și morale, dacă calitatea serviciului este afectată în detrimentul utilizatorului.

2.2. Consimțământul să fie specific

În strânsă legătură cu obligația de informare a operatorului și cerința privind „granularitatea”, un consimțământ dat pentru scopuri generale, nedefinite clar, nu poate fi considerat valid. În primul rând, îi revine operatorului de a identifica în mod clar scopurile pentru fiecare caz în parte. Conform art. 5 alin. (1) lit. (b) din Regulament, obținerea unui consimțământ valabil este întotdeauna precedată de determinarea unui scop specific, explicit și legitim pentru activitatea de prelucrare preconizată. Pentru aceste motive, un scop vag sau general, cum ar „fi îmbunătățirea experienței utilizatorilor”, „scopuri de marketing”, „scopuri de securitate IT” sau de „cercetare viitoare”, de obicei, nu îndeplinește criteriile de a fi specific[12].

Operatorii trebuie să furnizeze informații specifice, împreună cu fiecare cerere separată de consimțământ, referitoare la datele care sunt prelucrate în fiecare scop, pentru ca persoanele vizate să fie conștiente de impactul diferitelor opțiuni pe care le au la dispoziție[13]. Astfel, persoanele vizate au posibilitatea de a exprima un consimțământ specific.

În cazul în care consimțământul persoanei vizate este dat în contextul unei declarații scrise care se referă și la alte aspecte, cererea privind consimțământul trebuie să fie prezentată într-o formă care o diferențiază în mod clar de celelalte[14]. Prin adoptarea unor mecanisme de consimțământ detaliate, trebuie acordată posibilitatea persoanelor vizate de a-și da acordul separat pentru fiecare scop în parte sau doar pentru unele dintre ele.

Totuși, Regulamentul prevede o excepție, și anume cazul în care prelucrarea ulterioară are loc în scopuri de cercetare științifică sau istorică ori în scopuri statistice[15]; în acest caz, putem observa o serie de derogări, sub rezerva unor garanții adecvate pentru persoanele vizate[16].

[11] Grupul de lucru „Articolul 29”, Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, adoptate la 4 mai 2020, p. 9.

[12] Grupul de lucru „Articolul 29”, Opinia nr. 3/2013 privind limitarea scopului (WP 203), p. 16.

[13] Grupul de lucru „Articolul 29”, Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, adoptate la 4 mai 2020, p. 17.

[14] Art. 7 alin. (2) din Regulament.

[15] Considerentul (33) din Regulament.

[16] *I.A. Micu, Y. Beșleagă*, art. cit., p. 2.

2.3. Consimțământul să fie informat

În conformitate cu principiul transparenței[17], este nevoie de furnizarea informațiilor persoanelor vizate înainte de obținerea consimțământului, în lipsa căruia controlul utilizatorului devine iluzoriu. În acest sens, așa cum prevede și Comitetul european pentru protecția datelor, este esențială comunicarea cel puțin a următoarelor informații: identitatea operatorului, scopul fiecărei operațiuni de prelucrare pentru care se solicită consimțământul, tipul de date care vor fi colectate și utilizate, existența dreptului de retragere a consimțământului, informații privind utilizarea datelor pentru procesul decizional automatizat.

Informațiile și comunicările referitoare la prelucrare trebuie să fie ușor accesibile și facil de înțeles pentru orice persoană obișnuită, evitând politici de confidențialitate lungi și ilizibile și limbajul juridic[18]. În măsura în care informarea este redactată într-o limbă străină în mediul online, există posibilitatea ca nu toți vizitatori să cunoască limba respectivă; în acest caz, operatorul de date ar trebui să țină cont de limba fiecărei jurisdicții în care se află persoanele vizate, asigurând astfel informarea corectă a oricărei persoane[19].

De altfel, și art. 13 și 14 din Regulament indică informații minimale ce trebuie furnizate persoanelor vizate pentru obținerea consimțământului.

2.4. Consimțământul să fie neechivoc

Așa cum am menționat la începutul lucrării, caracterul neechivoc nu este o noutate absolută, însă Regulamentul este cel care explică semnificația acestuia. Regulamentul nu limitează exprimarea consimțământului doar la semnarea unei declarații, ci furnizează câteva exemple de manifestări de voință care pot fi privite ca un consimțământ valabil exprimat, ca, de exemplu, completarea unui formular electronic, bifarea unei casete, trimiterea unui e-mail, transmiterea unui document scanat și semnat de persoana vizată prin e-mail sau fax, încărcarea pe platforma operatorului a declarației purtând semnătura electronică a persoanei vizate, declarațiile orale (însă, în acest caz, poate fi dificilă dovedirea obținerii consimțământului)[20].

Așadar, consimțământul poate fi orice declarație sau un comportament care indică în mod clar voința persoanei vizate de a accepta prelucrările propuse, însă aceasta nu se extinde și la alte prelucrări.

Este de reținut faptul că Regulamentul prevede în mod clar că simpla abstențiune nu valorează consimțământ implicit, ceea ce înseamnă că metodele „opt – out" prin care persoana ale cărei date sunt colectate trebuie să debifeze o opțiune prebifată nu vor putea fi invocate drept mecanisme viabile[21].

În legătură cu consimțământul obținut în format electronic, Regulamentul specifică, în considerentul (32): „*în cazul în care consimțământul persoanei vizate trebuie acordat în urma unei cereri transmise pe cale electronică, cererea respectivă trebuie să fie clară și concisă și să nu perturbe în mod inutil utilizarea serviciului pentru care se acordă consimțământul*".

[17] Art. 5 alin. (1) din Regulament.

[18] *S. Crețu*, Consimțământul..., p. 32.

[19] Grupul de lucru „Articolul 29", Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, adoptate la 4 mai 2020, pp. 17-19.

[20] Considerentul (32) din Regulament.

[21] *Ibidem*.

Obținerea consimțământului prin platforme online, fără întreruperea activității utilizatorului, într-o anumită măsură, reprezintă o provocare, astfel, este nevoie de adoptarea metodelor care pot fi folosite cu ușurință. Potrivit cerințelor Regulamentului, operatorii au libertatea de a dezvolta un flux de obținere a consimțământului care se potrivește organizației lor. În acest sens, chiar și faptele fizice pot fi calificate ca o acțiune afirmativă clară în conformitate cu GDPR[22].

Glisarea pe ecran, a face cu mâna în fața unei camere smart, a învârti telefonul smart în sensul acelor de ceasornic sau în forma opt pot fi modalități prin care se manifestă acceptarea, atât timp cât sunt furnizate informații clare și este evident că fapta în cauză reprezintă acceptare pentru o anume solicitare[23].

Operatorul trebuie să poată demonstra că a fost obținut consimțământul în această modalitate și persoana vizată trebuie să poată să își retragă consimțământul la fel de ușor cum l-a exprimat.

Dimpotrivă, plimbarea cursorului în jos sau glisarea prin termenii și condițiile care includ declarația consimțământului, în situația în care pe ecran apare o alertă prin care i se aduce la cunoștință persoanei vizate că plimbarea cursorului în jos reprezintă consimțământ, nu satisface cerința unei acțiuni clare și afirmative. Asta se întâmplă, deoarece alerta poate fi omisă de către persoana vizată atunci când plimbă cursorul repede prin texte ample și o astfel de acțiune nu este suficient de clară[24].

În contextul digital, multe servicii au nevoie de datele cu caracter personal pentru a funcționa, deci persoanele vizate primesc o multitudine de cereri privind acordarea consimțământului în baza unui click sau a unei glisări, în fiecare zi. Aceasta poate rezulta într-o oarecare epuizare în urma click-urilor. Când este întâlnit de prea multe ori, efectul de prevenire propriu-zis al mecanismelor de acordare a consimțământului se diminuează[25].

În orice caz, este indicat să fie evitată forțarea persoanelor vizate să creeze conturi de utilizator și să se conecteze doar pentru a obține un consimțământ verificabil. Desigur, aceasta poate fi oferită ca opțiune, în cazul în care vizitatorii vor să-și salveze preferințele. Însă art. 11 din Regulament clarifică faptul că nu este nevoie de informații suplimentare pentru identificarea persoanei în vederea obținerii unei consimțământ valabil exprimat[26].

Dacă consimțământul urmează să fie colectat prin intermediul unei ecran mic sau într-o situație cu spațiu restrâns de informații, trebuie luată în considerare o modalitate de prezentare a informațiilor cât mai plăcută, pentru a evita perturbarea excesivă a experienței utilizatorilor sau a proiectării produsului[27].

Nu în ultimul rând, art. 7 alin. (1) din Regulament subliniază clar, obligația explicită a operatorului de a demonstra consimțământul persoanei vizate. Sarcina probei revine întotdeauna operatorului, conform considerentului (42), care prevede că: „*În cazul în care prelucrarea se bazează pe consimțământul persoanei vizate, operatorul ar trebui să fie în măsură să demonstreze faptul că persoana vizată și-a dat consimțământul pentru operațiunea de prelucrare*”.

[22] Grupul de lucru „Articolul 29”, Orientări asupra consimțământului în temeiul Regulamentului 2016/679, adoptate la 28 noiembrie 2017, p. 17.

[23] Grupul de lucru „Articolul 29”, Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, adoptate la 4 mai 2020, p. 22.

[24] *Ibidem*.

[25] *Ibidem*.

[26] Information Commissioner's Office, Guidance on the use of cookies and similar technologies. Documentul este disponibil online la adresa *https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf*, accesată în data de 11.03.2022, p. 32.

[27] Grupul de lucru „Articolul 29”, Orientări asupra consimțământului în temeiul Regulamentului 2016/679, adoptate la 28 noiembrie 2017, p. 14.

Evidența ținută de operator trebuie să conțină cel puțin următoarele elemente: cine a dat consimțământul (nume sau alt identificator), când a dat consimțământul (aceasta ar putea fi o dată tipărită pe o hârtie, o amprentă digitală sau data înregistrării consimțământului dat oral), ce fel de informații au fost furnizate (o copie a informațiilor furnizate persoanelor vizate în cazul în care consimțământul a fost exprimat în cadrul unei sesiuni online, înregistrarea declarațiilor orale ale persoanelor vizate obținute în timpul unui apel telefonic) și cum a fost obținut consimțământul (păstrarea unei evidențe a declarațiilor de consimțământ primite)[28].

Nu în ultimul rând, se recomandă reînnoirea consimțământului în mod periodic, la intervale de timp adecvate, astfel încât persoanele vizate să fie bine informate asupra modului în care datele lor sunt folosite și pentru a-și putea exercita în mod efectiv drepturile garantate de Regulament[29].

3. Obținerea consimțământului în practică

3.1. Obținerea consimțământului pentru trimitere „newsletter”

Internetul oferă un mediu indispensabil de căutare a informației, un mediu de comunicare, de socializare, de divertisment și, nu în ultimul rând, un mediu în care iau naștere afaceri profitabile. Există o mulțime de modalități de a ajunge la consumatori, de la chatbot și reclame plătite până la rețelele sociale și e-mailuri direcționate. Când sunt utilizate corect, campaniile de e-mail marketing, pot fi cea mai eficientă modalitate de comunicare cu potențialii clienți.

Pe măsură ce se apropia termenul-limită de 25 mai 2018 (momentul în care a început să se aplice Regulamentul), foarte multe dintre companii au început să trimită e-mailuri clienților în vederea reînnoirii consimțământului obținut înainte de GDPR, deși operatorii nu erau obligați în mod automat să reînnoiască în integralitate toate relațiile de consimțământ[30].

Conform considerentului (171) din Regulament, în cazul în care prelucrarea se bazează pe consimțământ în temeiul Directivei 95/46/CE, nu este necesar ca persoana vizată să își dea încă o dată consimțământul în cazul în care modul în care consimțământul a fost dat este în conformitate cu condițiile Regulamentului, astfel încât operatorului să i se permită să continue o astfel de prelucrare după data aplicării Regulamentului. Prin urmare, operatorii care sunt capabili să demonstreze obținerea de la persoane vizate a unui consimțământ valabil pentru operațiuni realizate în scop de marketing direct, inițiate pe tărâmul Directivei 95/46/CE, puteau să continue aceste operațiuni fără cereri de reînnoire a consimțământului[31].

Potrivit art. 12 din Legea nr. 506/2004[32] și art. 6 din Legea nr. 365/2002 privind comerțul electronic, republicată[33], este interzisă efectuarea de comunicări comerciale prin utilizarea unor sisteme automate

[28] One Trust, The Ultimate Consent Handbook for Privacy Professionals, 2018. Documentul este disponibil online la adresa *https://www.dataguidance.com/sites/default/files/20201228-onetrust-cookieconsent-handbook-digital.pdf*, accesată în data de 11.03.2022, p. 17.

[29] *I.A. Micu, Y. Beșleagă*, art. cit., p. 2.

[30] *K. Marcel*, 2 hónappal a GDPR után – Mi történt eddig?, 2018. Documentul este disponibil online la adresa *https://blog.crosssec.com/2-honappal-a-gdpr-utan-mi-tortent-eddig*, accesată in data de 28.03.2022.

[31] *M. Maxim*, Răspunderea civilă contractuală în domeniul protecției datelor cu caracter personal în contextul noului Regulament general (UE) privind protecția datelor nr. 2016/679, Ed. Universul Juridic, București, 2021, p. 76.

[32] Publicată în M. Of. nr. 1101 din 25 noiembrie 2004.

[33] Republicată în M. Of. nr. 959 din 29 noiembrie 2006.

de apelare și comunicare, prin fax sau poștă electronică sau orice altă metodă care folosește servicii de comunicații electronice destinate publicului, cu excepția cazului în care destinatarul și-a exprimat, în prealabil, în mod expres consimțământul pentru a primi astfel de notificări.

Cu toate acestea, înainte de aplicarea Regulamentului, era o practică comună achiziționarea bazelor de date și obținerea datelor de contact ale utilizatorilor prin folosirea casetelor bifate automat la crearea unui cont, prin care operatorii de date obțineau consimțământul pasiv al utilizatorilor pentru a trimite mesaje de marketing.

Mai mult, pe piața serviciilor, în special în sectorul telecomunicațiilor, s-a întâmplat, de multe ori, ca adresele de e-mail sau numerele de telefon ale persoanelor vizate furnizate la încheierea contractului să fie utilizate în scopuri de marketing fără a se solicita consimțământul sau fără ca utilizatorul să fie informat în prealabil.

Odată cu intrarea în vigoare a Regulamentului însă, s-au schimbat în mod fundamental regulile jocului în acest domeniu.

În primul rând, Regulamentul stabilește, prin considerentul (32), că „*consimțământul ar trebui acordat printr-o acțiune neechivocă care să constituie o manifestare liber exprimată, specifică, în cunoștință de cauză și clară a acordului persoanei vizate pentru prelucrarea datelor sale cu caracter personal*”. Așadar, mecanismele de obținere a consimțământului de tipul „opt – out” (prin care persoana vizată trebuie sa debifeze o opțiune prebifată în cazul în care nu dorește să îi fie prelucrate datele) nu pot fi considerate valabile, la fel cum nici impunerea unor termeni comerciali abuzivi, fără altă opțiune, nu poate servi la demonstrarea obținerii consimțământului pentru prelucrarea datelor în scopuri subsecvente celui implicat de art. 6 alin. (1) lit. (b) din Regulament[34)].

În al doilea rând, Regulamentul impune companiilor să demonstreze modul în care a fost obținut consimțământul. Regulamentul introduce cerințe pentru operatori de a lua măsuri suplimentare în scopul de a se asigura că obțin, păstrează și pot demonstra existența consimțământului valabil. În acest sens, art. 7 din Regulament cuprinde dispoziții specifice referitoare la păstrarea evidenței privind consimțământul.

O metodă eficientă mult folosită în practică pentru constatarea existenței reale a consimțământului este verificarea în două etape. De exemplu, la momentul transmiterii primei comenzi pe un site, clientul are posibilitatea de a bifa, printr-un click, opțiunea de a primi periodic, la adresa indicată pentru livrarea produselor, un newsletter cu oferte personalizate. Totodată, operatorul îi transmite persoanei vizate pe e-mail un link de verificare pe care aceasta trebuie să îl acceseze sau un SMS cu un cod de verificare, pentru confirmarea acordului la abonare[35)].

Din practica Autorității Naționale de Supraveghere privind protecția datelor cu caracter personal (în continuare, „ANSPDCP”), putem observa că consimțământul persoanei vizate este unul dintre cele mai des întâlnite subiecte, din cauza faptului că foarte mulți operatori trimit comunicări în scop de marketing, așa-zisele *newsletters*, fără a avea consimțământul prealabil al persoanei vizate.

În România sunt mai multe cazuri în care ANSPDCP a aplicat amenzi pentru nerespectarea criteriilor prevăzute de Regulament.

În luna august a anului 2019, în urma investigațiilor realizate de ANSPDCP, a fost constatat faptul că operatorul INTELIGO MEDIA S.A. (*avocatnet.ro*) a folosit o metodă abuzivă de obținere a consimțământului prin folosirea unei căsuțe nebifate cu următorul conținut: „Nu vreau să primesc «personal update»,

[34)] Art. 6 alin. (1) lit. (b) din Regulament prevede ipoteza în care prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri, la cererea persoanei vizate, înainte de încheierea unui contract.

[35)] *I.A. Micu, Y. Beșleagă*, art. cit., p. 2.

informarea trimisă zilnic, gratuit, pe e-mail, de avocatnet.ro". Potrivit acestor condiții stabilite de operator, în măsura în care un utilizator a omis bifarea acestei căsuțe, a fost automat abonat, respectiv e-mailul său a fost introdus în baza de abonați. Astfel, abonarea a avut loc în absența unei manifestări de voință din partea utilizatorilor, care să indice în mod clar acceptarea prelucrării în scopul stabilit de operator. Din punctul de vedere al ANSPDCP, operatorul nu a putut face dovada obținerii unui consimțământ valabil, conform GDPR, pentru prelucrarea datelor cu caracter personal ale unui număr de 4.357 abonați. De asemenea, pentru transmiterea prin e-mail a informării zilnice, operatorul a prelucrat datele în baza unui temei legal neadecvat scopului, respectiv „executarea unui contract". Amenda aplicată în acest caz a fost 9.000 euro[36].

De asemenea, societatea Orange România SA a primit prima amendă pentru nerespectarea legislației privind protecția datelor încă din anul 2018, pe baza Legii nr. 677/2001. Astfel, prin decizia din 2018, ANSPDCP a constatat că operatorul a stocat copii ale actelor de identitate ale clienților săi fără să demonstreze că acești clienți își dăduseră consimțământul în mod valabil. În decizia sa, ANSPDCP a arătat că, în perioada cuprinsă între 1 și 26 martie 2018, Orange România a încheiat contracte de furnizare a unor servicii de telecomunicații mobile cu persoane fizice și că la respectivele contracte erau anexate copiile actelor de identitate ale acestor persoane. Potrivit ANSPDCP, societatea nu a făcut dovada faptului că clienții săi, ale căror contracte aveau anexate copii ale actelor lor de identitate, își dăduseră consimțământul cu privire la colectarea și la stocarea unor copii ale actelor lor de identitate. Împotriva acestei decizii, Orange România a introdus o contestație la Tribunalul București. Cauza a ajuns până la Curtea Europeană de Justiție, unde Curtea, în decizia sa, a statuat că operatorului de date îi revine sarcina să demonstreze că persoana vizată și-a manifestat, prin intermediul unui comportament activ, consimțământul pentru prelucrarea datelor sale cu caracter personal și că aceasta a obținut în prealabil o informare cu privire la toate circumstanțele aferente acestei prelucrări, într-o formă inteligibilă și ușor accesibilă, precum și utilizând un limbaj clar și simplu, care să-i permită să determine cu ușurință consecințele acestui consimțământ, astfel încât să se garanteze că acesta este dat în deplină cunoștință de cauză. Un contract privind furnizarea de servicii de telecomunicații care conține o clauză potrivit căreia persoana vizată a fost informată și a dat consimțământul pentru colectarea, precum și pentru stocarea unei copii a actului său de identitate, în scop de identificare, nu este de natură să demonstreze că această persoană și-a dat în mod valabil consimțământul:

- atunci când căsuța care se referă la această clauză a fost bifată de operatorul de date anterior semnării acestui contract sau
- atunci când clauzele contractului menționat sunt de natură să inducă persoana vizată în eroare cu privire la posibilitatea de a încheia contractul în discuție în pofida refuzului de a-și da consimțământul pentru prelucrarea datelor sale sau
- atunci când libera alegere de a se opune acestei colectări și acestei stocări este afectată în mod nejustificat de acest operator prin cerința ca, pentru a refuza să își dea consimțământul, persoana vizată să completeze un formular suplimentar în care să fie menționat acest refuz[37].

Deși, în acest caz, amenda a fost aplicată înainte de intrarea în vigoare a Regulamentului, din hotărârea Curții reiese importanța implementării măsurilor tehnice și organizatorice prin care operatorul este capabil să demonstreze conformarea cu cerințele normelor privind protecția datelor cu caracter personal.

Un alt incident a fost constatat de ANSPDCP în anul 2021. În fapt, operatorul BNP Paribas Personal Finance SA a fost sancționat cu 10.000 lei pentru că nu a făcut dovada existenței consimțământului prealabil

[36] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Alta_sanctiune_RGPD&lang=ro*, accesată în data de 24.02.2022.

[37] Cauza C-61/19, *Orange România SA împotriva Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP)*, ECLI:EU:C:2020:901.

al persoanei vizate. În fapt, persoana vizată a primit pe telefon mesaje comerciale de tip SMS din partea operatorului, cu toate că și-a exercitat, în repetate rânduri, dreptul de opoziție față de aceste prelucrări, motiv pentru care a reclamat aspectul către ANSPDCP[38]. Ca urmare a finalizării investigației, ANSPDCP a aplicat amenda, motivând că operatorul în cauză a încălcat prevederile dispozițiile art. 12 din Legea nr. 506/2004.

Oferirea posibilității de retragere a consimțământului este la fel de importantă ca obținerea consimțământului valabil exprimat.

Conform art. 7 alin. (3) din Regulament: „*Persoana vizată are dreptul să își retragă în orice moment consimțământul. Retragerea consimțământului nu afectează legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia. Înainte de acordarea consimțământului, persoana vizată este informată cu privire la acest lucru. Retragerea consimțământului se face la fel de simplu ca acordarea acestuia*".

Înainte de a-și da consimțământul, persoana vizată trebuie informată despre existența dreptului de retragere, despre faptul că retragerea va afecta numai prelucrarea ulterioară și, ca o bună practică, și despre modul în care poate să retragă consimțământul. Operatorul trebuie să asigure metode la fel de ușoare pentru retragerea consimțământului ca și cele în care a fost acordat. De exemplu, pot fi folosite instrumentele de gestionare a preferințelor sau dashboards de confidențialitate. Dacă consimțământul este dat printr-un singur mijloc, persoana vizată ar trebui să poată folosi același mijloc pentru a-și retrage consimțământul[39].

Autoritatea Națională de Supraveghere privind protecția datelor cu caracter personal, în foarte multe cazuri, a aplicat amenzi pentru încălcarea prevederilor privind retragerea consimțământului. În anul 2021, Telekom România Communications S.A. a fost sancționată cu avertisment ca urmare a constatării faptului că a prelucrat date în scop de marketing, deși nu avea un temei legal în acest sens, încălcând prevederile art. 6 din Regulament. În fapt, o persoană vizată, fost client al Telekom, odată cu încetarea relației contractuale, a menționat că își retrage consimțământul și nu mai dorește să primească informări cu privire la serviciile operatorului.

Cu toate acestea, operatorul a contactat persoana vizată, care și-a exercitat dreptul de opoziție și a solicitat ștergerea numărului său de telefon și adresa de e-mail din baza de date a Telekom. În mod accidental (operatorul a menționat că ar fi fost vorba de o eroare umană), din nou, Telekom contactează persoana vizată în scop de marketing. Persoana vizată a făcut iarăși o solicitare de a nu mai fi contactat și de a i se șterge datele din baza de date Telekom.

Pe lângă avertisment, pentru că operatorul a contactat telefonic o persoană care și-a exercitat dreptul de opoziție față de astfel de prelucrări, Telekom a fost sancționat și cu 2.000 euro, încălcând prevederile art. 21 din Regulament[40].

De asemenea, societatea Dante International (administratorul eMAG) a fost amendată cu 3.000 euro, pentru că, la sfârșitul anului 2019, a trimis unei persoane fizice un mesaj comercial, deși aceasta a solicitat ștergerea adresei de e-mail din baza de date a operatorului, deoarece a fost obținută fără acordul său. Astfel, obiectul amenzii a fost trimiterea de mesaje comerciale nesolicitate, fără a avea consimțământul persoanei vizate[41].

[38] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Amenda_pentru_incalcarea_RGPD&lang=ro*, accesată în data de 24.02.2022.

[39] One Trust, The Ultimate Consent Handbook for Privacy Professionals, 2018. Documentul este disponibil online la adresa *https://www.dataguidance.com/sites/default/files/20201228-onetrust-cookieconsent-handbook-digital.pdf*, accesată în data de 11.03.2022, p. 17.

[40] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Comunicat_Presa_06_12_2021_2&lang=ro*, accesată în data de 30.03.2022.

[41] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Comunicat_amenda_dante_international_martie_2020&lang=ro*, accesată în data de 30.03.2022.

O cauză similară a avut și operatorul Artmark Holding SRL, care nu a dat curs cereri persoanei vizate, continuând să îi trimită mesaje comerciale de tip SPAM. Autoritatea a clasificat aceste acțiuni abuzive și contrare principiilor protejării datelor cu caracter personal. Amenda de 10.000 lei a venit însoțită și cu îndrumări și recomandări către operator[42)].

De asemenea, Elefant Online S.A. nu a putut face dovada obținerii consimțământului prealabil expres și neechivoc pentru transmiterea de mesaje comerciale prin e-mail. Mai mult decât atât, persoana vizată a continuat să primească astfel de mesaje și după dezabonarea (prin 2 metode) de la astfel de servicii. Astfel, ANSPDCP a aplicat o amendă contravențională, în valoare de 10.000 lei[43)].

Așa cum putem observa, ANSPDCP ne oferă exemple importante cu privire la folosirea în mod abuziv a adresei de e-mail și importanța respectării drepturilor persoanelor vizate.

3.2. Obținerea consimțământului pentru utilizarea modulelor cookie pe pagina web

Pe măsură ce tehnologia a evoluat, a devenit necesară utilizarea unor noi tehnici pentru promovarea produselor și serviciilor. În loc de e-mailuri simple în căsuța poștală, companiile folosesc din ce în ce mai mult reclame direcționate, care sunt afișate utilizatorilor pe baza activităților efectuate în mediul online.

În prezent, aproape toate site-urile web utilizează în mod obișnuit module cookie pentru a urmări activitatea online a vizitatorilor, pentru a genera statistici și, în general, pentru a menține funcționarea website-ului.

„Cookie-uri" sunt fișiere de mici dimensiuni, formate din litere și numere, care sunt stocate pe calculator, terminalul mobil sau alte echipamente de pe care se accesează un website. Un cookie este instalat prin solicitarea emisă de către un web-server unui browser (de exemplu: Internet Explorer, Chrome), care stochează informații cu privire la activitatea utilizatorilor pe respectivele site-uri cum ar fi: paginile accesate sau perioada petrecută pe o anumită pagină[44)].

Fișierele de tip cookie permit recunoașterea echipamentului utilizatorului și afișarea în mod corespunzător a paginii de Internet, adaptată preferințelor individuale ale utilizatorului. Astfel, fișierele de tip cookie contribuie la crearea unei experiențe de navigare web simple și personalizate, în funcție de interesele, preferințele și comportamentul fiecărui utilizator.

Prin raportare la criteriul duratei de valabilitate, fișierele de tip cookie se clasifică în cookie-uri de sesiune, care se instalează în terminalul utilizatorului în timpul vizitei pe website și rămâne acolo până la închiderea sesiunii sau a browser-ului folosit, și cookie-uri permanente, care rămân în terminalul utilizat pentru o perioadă de timp mai mare, în funcție de parametrii acestora sau până când sunt șterse manual[45)].

După criteriul proveniență, fișierele de tip cookie se clasifică în fișiere generate și folosite de către website-ul principal (*First Party*) și fișiere create de terți (*Third Party*).

[42)] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Comunicat_Presa_Amenda_Artmark&lang=ro*, accesată în data de 30.03.2022.

[43)] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Amenda_Elefant_Online&lang=ro*, accesată în data de 30.03.2022.

[44)] *J. Schwartz*, 'Giving Web a Memory Cost Its Users Privacy'. Documentul este disponibil online la adresa *www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html*, accesată în data de 11.03.2022.

[45)] Information Commissioner's Office, Guidance on the use of cookies and similar technologies. Documentul este disponibil online la adresa *https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf*, accesată în data de 11.03.2022.

În ceea ce privește funcționalitatea, există mai multe tipuri de module cookie, a căror clasificare cea mai comună este prezentată în Ghidul publicat de Camera de Comerț Internațională Britanică[46], ghid care este relevant pentru stabilirea normelor care se aplică în cazul folosirii cookie-urilor. Conform acestui ghid, se face distincția între:

- cookie-uri strict necesare, care permit navigarea pe site-ul web. Fără aceste module cookie, este imposibil să se furnizeze conținutul site-ului (inclusiv utilizarea protocoalelor securizate). Această categorie include, de exemplu, a) așa-numitele «cookie-uri de sesiune», care sunt utilizate pentru a urmări datele introduse de utilizator în timpul comunicării cu furnizorul de servicii. De obicei, site-urile web utilizează propriile module cookie, care se bazează pe un identificator de sesiune (un număr de identificare temporară aleatoriu) și expiră cel târziu la sfârșitul sesiunii; b) cookie-uri de autentificare, care sunt utilizate pentru a identifica utilizatorul la autentificare (de exemplu, la autentificarea într-un cont privat). Aceste module cookie permit utilizatorilor să se identifice în timpul vizitelor pe site-ul web și să acceseze conținutul autorizat; c) cookie-uri de securitate, care sunt utilizate pentru a detecta încercările repetate de conectare eșuate la site-ul web sau sunt concepute pentru a proteja împotriva altor abuzuri ale sistemului de conectare.
- cookie-urile de performanță colectează informații despre modul în care vizitatorii utilizează un site web, de exemplu, ce pagini sunt vizitate cel mai des și/sau dacă utilizatorul întâmpină mesaje de eroare. De regulă, cookie-urile de performanță sunt folosite pentru a îmbunătăți modul în care funcționează website-ul.
- cookie-urile privind funcționalitatea înregistrează alegerile pe care utilizatorul le face, cum ar fi: limba preferată, dimensiunea caracterelor și oferă utilizatorului caracteristici personalizate de folosire a site-ului.
- cookie-urile pentru analiza web și direcționarea publicității permit site-urilor web să construiască profiluri comportamentale ale utilizatorilor și să afișeze reclame personalizate, pe baza intereselor individuale ale acestora. Informațiile colectate pentru monitorizarea comportamentului pot fi utilizate pentru a urmări o serie de activități online, cum ar fi ceea ce citesc, urmăresc sau caută utilizatorii sau chiar pentru a le determina locația exactă.

Identificatorul anonim și unic din conținutul cookie-urilor este, de obicei, suficient pentru îndeplinirea scopului (memorarea și setarea automată a funcțiilor site-ului web, colectarea de date statistice sau chiar afișarea de reclame direcționate), însă acest lucru nu înseamnă că utilizarea cookie-urilor nu este un mecanism eficient pentru urmărirea utilizatorilor, chiar dacă informațiile colectate sunt utilizate fără ca numele vizitatorului să fie cunoscut. „Persoanele fizice pot fi asociate cu identificatorii online furnizați de dispozitivele, aplicațiile, instrumentele și protocoalele lor, cum ar fi adresele IP, identificatorii cookie sau alți identificatori (...). Aceștia pot lăsa urme care, în special atunci când sunt combinate cu identificatori unici și alte informații primite de servere, pot fi utilizate pentru crearea de profiluri ale persoanelor fizice și pentru identificarea lor”[47].

Cu toate acestea, este important de subliniat faptul că nu toate informațiile generate cu ajutorul modulelor cookie (sau al altor tehnologii similare) pot identifica efectiv o persoană, chiar și indirect. Prin urmare, nu se poate spune, în general, că toate modulele cookie ar trebui să fie considerate identificatori online sau că informațiile colectate prin utilizarea lor sunt întotdeauna date cu caracter personal.

În primul rând, protejarea confidențialității comunicațiilor în cazul concret al utilizării de module cookie și dispozitive similare este prevăzută, în principal, de art. 5 alin. (3) din Directiva 2002/58/CE, astfel cum

[46] International Chamber of Commerce, ‘ICC UK Cookie guide’. Documentul este disponibil online la adresa *www.huntingact.org/wp-content/uploads/icc-uk-cookie-guide.pdf*, accesată în data de 11.03.2022.

[47] Considerentul (30) din Regulament.

a fost modificată prin Directiva 2009/136/CE[48], care prevede că: „*Statele membre se asigură că stocarea de informații sau dobândirea accesului la informațiile deja stocate în echipamentul terminal al unui abonat sau utilizator este permisă doar cu condiția ca abonatul sau utilizatorul în cauză să își fi dat acordul, după ce a primit informații clare și complete, în conformitate cu Directiva 95/46/CE, inter alia, cu privire la scopurile prelucrării. Aceasta nu împiedică stocarea sau accesul tehnic cu unicul scop de a efectua transmisia comunicării printr-o rețea de comunicații electronice sau în cazul în care acest lucru este strict necesar în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator*”.

Astfel, putem observa că Directiva 2002/58/CE impune obținerea consimțământului în cunoștință de cauză în vederea stocării de informații în mod legal sau a obținerii accesului la informațiile stocate în echipamentul terminal al unui abonat sau utilizator, cu excepția cazului în care prelucrarea acestor informații este strict necesară în vederea furnizării unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.

În cazul în care, ca urmare a introducerii și recuperării informațiilor prin intermediul modulelor cookie sau al unor dispozitive similare, informațiile colectate sunt considerate date cu caracter personal, pe lângă art. 5 alin. (3) mai sus menționat, se aplică și Regulamentul privind protecția datelor cu caracter personal, care însă nu stabilește în mod direct necesitatea obținerii consimțământului în vederea prelucrării informațiilor stocate de modulele cookie, lăsând la latitudinea operatorului să aleagă unul dintre temeiurile legale prevăzute de art. 6 din Regulament.

Astfel, în situația aplicării ambelor norme, se ridică problema stabilirii dispozițiilor aplicabile fiecăreia dintre ele[49].

În acest sens, vom avea în vedere considerentul (173) din Regulament, care prevede că: „*Prezentul regulament ar trebui să se aplice tuturor aspectelor referitoare la protecția drepturilor și libertăților fundamentale legate de prelucrarea datelor cu caracter personal, care nu fac obiectul unor obligații specifice cu același obiectiv ca cel stabilit în Directiva 2002/58/CE a Parlamentului European și a Consiliului, inclusiv obligațiile privind operatorul și drepturile persoanelor fizice*”.

Vom observa că art. 5 alin. (3) din Directiva asupra confidențialității și comunicațiilor electronice, care se referă la consimțământul în cunoștință de cauză, este aplicabil în mod direct, având în vedere o aplicare a doctrinei conform căreia o lege care reglementează o problemă specifică (*lex specialis*) are prioritate asupra unei legi care reglementează o problemă generală (*lex generalis*), Directiva fiind o lege specială, în acest caz, în sectorul comunicațiilor electronice.

Nu în ultimul rând, trebuie să discutăm și cazul în care informațiile colectate prin intermediul modulelor cookie sunt date cu caracter personal, dar regulile prevăzute în Directivă nu se aplică, având în vedere că acesta cade sub excepția prevăzută în Directivă și prelucrarea este strict necesară în vederea furnizării de către furnizor a unui serviciu al societății informaționale cerut în mod expres de către abonat sau utilizator.

Conform Orientărilor Grupului de lucru, următoarele cookie-uri pot fi scutite de obținerea consimțământului în cunoștință de cauză în anumite condiții, dacă nu sunt utilizate în alte scopuri:

1) cookie-urile de înregistrare a inputului utilizatorului *(session-id)*, pe durata unei sesiuni, sau cookie-urile persistente, limitate la câteva ore în anumite cazuri;

[48] Directiva 2009/136/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivei 2002/22/CE privind serviciul universal și drepturile utilizatorilor cu privire la rețelele și serviciile de comunicații electronice, a Directivei 2002/58/CE privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice și a Regulamentului (CE) nr. 2006/2004 privind cooperarea dintre autoritățile naționale însărcinate să asigure aplicarea legislației în materie de protecție a consumatorului, publicată în J. Of., seria L, nr. 337 din 18 decembrie 2009.

[49] Grupul de lucru „Articolul 29”, Avizul nr. 2/2010 privind publicitatea comportamentală online, adoptat la 22 iunie 2010, pp. 10-11.

2) cookie-urile de autentificare, utilizate pentru servicii autentificate, pe întreaga durată a unei sesiuni;

3) cookie-urile de securitate centrate pe utilizator, utilizate pentru a detecta abuzurile legate de autentificare, persistente, dar limitate în timp;

4) cookie-urile de sesiune ale playerelor multimedia, cum ar fi cookie-urile flash, pe întreaga durată a unei sesiuni;

5) cookie-urile de sesiune pentru echilibrarea încărcării, pe întreaga durată a sesiunii;

6) cookie-urile persistente de personalizare a interfeței de utilizator, pe întreaga durată a unei sesiuni (sau pentru puțin mai mult timp);

7) cookie-urile de terță parte de schimb de conținut ale plugin-urilor sociale, pentru membrii conectați ai unei rețele sociale[50].

Cu toate acestea, este important de remarcat faptul că utilizările cookie-urilor sunt atât de diverse, încât, în multe cazuri, este imposibil să le clasificăm în mod clar.

Atunci când, conform Directivei, nu este necesar consimțământul pentru folosirea cookie-urilor necesare, vom apela la normele prevăzute de GDPR, care menționează un total de șapte temeiuri legale din care operatorul este liber să aleagă. Desigur, consimțământul poate fi, de asemenea, un temei juridic adecvat în acest caz, dar, în cazul în care sunt îndeplinite celelalte condiții, operatorul poate folosi una dintre celelalte temeiuri legale.

3.3. Obținerea consimțământului la locul de muncă

Conform art. 38 teza I C.muncii, „*salariații nu pot renunța la drepturile ce le sunt recunoscute prin lege*”, implicit nici la dreptul de protecție împotriva prelucrării nelegale a datelor sale personale.

Regulamentul subliniază nevoia de a proteja interesele specifice ale angajaților și prevede că „*statele membre pot prevedea norme mai detaliate pentru a asigura protecția drepturilor și a libertăților cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă, în special în scopul recrutării, al îndeplinirii clauzelor contractului de muncă, inclusiv descărcarea de obligațiile stabilite prin lege sau prin acorduri colective, al gestionării, planificării și organizării muncii, al egalității și diversității la locul de muncă, al asigurării sănătății și securității la locul de muncă, al protejării proprietății angajatorului sau a clientului, precum și în scopul exercitării și beneficierii, în mod individual sau colectiv, de drepturile și beneficiile legate de ocuparea unui loc de muncă, precum și pentru încetarea raporturilor de muncă*”[51].

Anterior aplicării Regulamentului general privind protecția datelor, consimțământul salariatului pentru prelucrarea datelor sale cu caracter personal a fost un temei mult utilizat în practică de către angajatorii din România. Așa cum putem observa din practică, încă o serie de operatori încearcă sa dovedească respectarea prevederilor Regulamentului prin faptul că au obținut documente semnate de angajați prin care aceștia au exprimat acordul privind prelucrarea datelor care îi privesc.

Deși, la prima vedere, ar părea că acesta este cel mai facil temei pentru prelucrarea datelor personale ale angajatului, se pune problema raportului de forțe inegal dintre angajat și angajator. Având în vedere dependența care rezultă din relația dintre angajator și angajat, există un dezechilibru de putere fiind puțin probabil ca persoana vizată să poată refuza să-și acorde consimțământul față de angajatorul său fără a se

[50] Grupul de lucru „Articolul 29”, Avizul nr. 04/2012 cu privire la exceptările de la consimțământul privind modulele cookie, adoptat la 7 iunie 2012, pp. 12-13.

[51] Art. 88 alin. (1) din Regulament.

confrunta cu temerea sau cu riscul real de consecințe negative ca urmare a unui refuz. Astfel, este foarte dificil ca angajatorii să prelucreze datele personale ale angajaților actuali sau viitori pe baza consimțământului, întrucât este puțin probabil ca acesta să fie acordat în mod liber[52].

Astfel, clauzele din contractul de muncă prin care salariatul își exprimă acordul cu privire la prelucrarea tuturor datelor personale sau a unei categorii de date sunt lovite de nulitate absolută.

De asemenea, în opinia Grupului de lucru pentru protecția datelor instituit în temeiul articolului 29: *„acolo unde prelucrarea datelor este necesară și reprezintă o consecință inevitabilă a raporturilor de muncă, un angajator se înșală atunci când încearcă să justifice această prelucrare pe baza consimțământului. Folosirea consimțământului de către angajator ar trebui să se limiteze la cazurile în care angajatul are o reală libertate de alegere și poate să-și retragă consimțământul fără a fi prejudiciat"*[53].

Mai mult, în cuprinsul Opiniei nr. 15/2011 a Grupului de lucru „Articolul 29", este evidențiat faptul că, în cazul în care persoana vizată se află sub influența operatorului de date, cum ar fi o relație de muncă, din cauza naturii relației sau a circumstanțelor speciale, aceasta ar putea să se teamă că ar putea fi tratată diferit dacă nu acceptă prelucrarea datelor[54].

Însă aceasta nu înseamnă că angajatorii nu pot să se bazeze niciodată pe consimțământul angajaților ca bază legală pentru prelucrarea datelor. Pot exista situații când angajatorul poate demonstra că acordarea consimțământului a fost făcută fără a exista vreun element de constrângere, presiune sau incapacitate de a-și exprima voința în mod liber[55].

În acest sens, Grupul de lucru „Articolul 29" ne oferă următorul exemplu: *„Un echipaj de filmare urmează să filmeze într-o anume parte dintr-un birou. Angajatorul cere tuturor angajaților care își desfășoară activitatea în acea parte consimțământul de a fi filmați, deoarece aceștia ar putea să apară pe fundalul filmării. Cei care nu vor să fie filmați nu sunt sancționați sub nicio formă, dar, în schimb, le sunt oferite munci echivalente în altă parte a clădirii pe durata filmărilor"*[56].

În relațiile de muncă, consimțământul, ca temei legal al prelucrării, este folosit destul de des pentru a activa sisteme de monitorizare, cum ar fi camerele de supraveghere la locul de muncă. Acest lucru este cu atât mai deranjant pentru persoanele vizate cu cât există cazuri în care se fac, fără nicio informare, înregistrări audio-video prin diverse sisteme.

Astfel, utilizarea camerelor de supraveghere video reprezintă unul dintre cele mai problematice și contestate aspecte în relațiile de muncă, ceea ce putem observa și din practica autorităților.

În concret, în anul 2019, ANSPDCP a efectuat o investigație la operatorul Glove Technology SRL, care a instalat camere de supraveghere audio-video în birourile angajaților (deci la locul de muncă), fără a își duce la îndeplinire obligațiile de legalitate, echitabilitate și transparență (adică nu avea temei legal – nu exista consimțământ, nu a avut un test de proporționalitate și nici nu a făcut informarea persoanelor vizate). Totodată, firma a montat aceste camere audio-video pentru a folosi informațiile colectate la o dată ulterioară, împotriva angajaților.

---

[52] Grupul de lucru „Articolul 29", Orientările 05/2020 privind consimțământul în temeiul Regulamentului 2016/679, adoptate la 4 mai 2020, p. 10.

[53] Grupul de lucru „Articolul 29", Avizul nr. 8/2001 privind prelucrarea datelor personale în contextul ocupării forței de muncă, p. 3.

[54] Grupul de lucru „Articolul 29", Avizul nr. 15/2011 privind definiția consimțământului, p. 14.

[55] *I.A. Micu, Y. Beșleagă*, art. cit., p. 2.

[56] Grupul de lucru „Articolul 29", Orientări asupra consimțământului în temeiul Regulamentului 2016/679, adoptate la 28 noiembrie 2017, p. 7.

Astfel, ANSPDCP, pe lângă aplicarea unei amenzi de 5.000 euro, a pus în vedere operatorului să înceteze orice operațiune de monitorizare prin acest sistem, să șteargă orice evidențe ale înregistrărilor prin sistemul dat și să asigure conformitatea sa[57].

Într-o altă cauză, în 2019, PRICEWATERHOUSECOOPERS BUSINESS SOLUTIONS S.A. (PwC) a fost amendată cu 150.000 euro pentru aplicarea bazei legale necorespunzătoare și încălcarea principiului răspunderii de către o companie.

Conform comunicatului, Autoritatea elenă pentru protecția datelor a efectuat o investigație privind legalitatea procesării datelor cu caracter personal ale angajaților companiei, care reclamaseră faptul că au fost obligați să-și acorde consimțământul pentru prelucrarea datelor lor personale de către operator. Autoritatea a constatat că operatorul în cauză a prelucrat în mod ilegal datele cu caracter personal ale angajaților săi, contrar dispozițiilor art. 5 alin. (1) lit. (a) din Regulament, deoarece a folosit un temei legal necorespunzător.

Totodată, acesta a prelucrat datele personale ale angajaților săi, contrar dispozițiilor art. 5 alin. (1) lit. (a), (b) și (c) din Regulament, spunând că prelucrează date în baza consimțământului, în conformitate cu art. 6 alin. (1) lit. (a) din Regulament, în timp ce, în realitate, prelucrau datele lor sub o bază legală diferită, despre care angajații nu au fost niciodată informați.

Deși era responsabilă în calitatea sa de operator, PwC nu a putut demonstra conformitatea cu art. 5 alin. (1) din Regulament, încălcând principiul răspunderii, prevăzut la art. 5 alin. (2) din Regulament, prin transferarea sarcinii dovezii de conformitate către persoanele vizate. Astfel, autoritatea a impus măsuri corective și sancțiuni administrative[58].

După cum observăm din practică, folosirea consimțământului angajaților pentru instalarea camerelor de supraveghere video la locul de muncă nu constituie o bază legală potrivită. Este nevoie mai degrabă de demonstrarea interesului legitim al operatorului.

Art. 5 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului[59] tratează în mod expres interesul legitim al angajatorului în utilizarea sistemelor de monitorizare prin mijloace de comunicații electronice și/sau prin mijloace de supraveghere video la locul de muncă și, în consecință, prelucrarea datelor cu caracter personal ale angajaților.

Prelucrarea datelor în baza interesului legitim implică o serie de obligații pentru operatorul de date și este permisă numai dacă:

a) interesele legitime urmărite de angajator sunt temeinic justificate și prevalează asupra intereselor sau drepturilor și libertăților persoanelor vizate;

b) angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților;

c) angajatorul a consultat sindicatul sau, după caz, reprezentanții angajaților înainte de introducerea sistemelor de monitorizare;

d) alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu și-au dovedit anterior eficiența; și

[57] ANSPDCP, Comunicat de presă. Documentul este disponibil online la adresa *https://www.dataprotection.ro/?page=Comunicat_Presa_21.10.2021_2&lang=ro*, accesată în data de 24.03.2022.

[58] *Cr.-Șt. Donciu*, PwC amendată cu 150.000 EUR pentru nerespectarea GDPR!. Documentul este disponibil online la adresa *https://dpo-net.ro/pwc-amendata-pentru-nerespectarea-gdpr/?fbclid=IwAR0VmthIt9uBJdTJnfLiiAL4ApKnO1E4l-_3U5R1l46i73WqaeQM00MuHEA*, accesată în data de 13.03.2022.

[59] Publicată în M. Of. nr. 651 din 26 iulie 2018.

e) durata de stocare a datelor cu caracter personal este proporțională cu scopul prelucrării, dar nu mai mare de 30 de zile, cu excepția situațiilor expres reglementate de lege sau a cazurilor temeinic justificate[60].

4. Concluzii

Având în vedere toate cele prezentate, putem concluziona că identificarea și implementarea mecanismelor care asigură obținerea unui consimțământ valid reprezintă o sarcină dificilă.

În primul rând, Internetul lucrurilor și rețelele electrice inteligente creează provocări privind confidențialitatea și protecția datelor cu caracter personal. În acest context, consimțământul rămâne un mijloc important de control al datelor cu caracter personal pentru persoane vizate, de aceea obținerea corectă a acestuia devine din ce în ce mai importantă. Controlul persoanelor vizate asupra modului în care sunt prelucrate datele cu caracter personal care le aparțin trebuie să fie efectiv, și nu doar iluzoriu, fiind esențială respectarea tuturor condițiilor prevăzute de Regulament, astfel cum sunt clarificate și detaliate și în Orientările Grupului de lucru „Articolul 29".

În al doilea rând, chiar și în ipoteza în care consimțământul persoanelor vizate este temeiul prelucrării, aceasta nu presupune o libertate mai mare pentru operator în privința modului în care alege să prelucreze datele. Faptul că persoanele vizate și-au dat acordul la prelucrare nu conduce la atenuarea rigorii celorlalte obligații ale operatorului, acesta fiind în continuare ținut să respecte limitările legate de scopul prelucrării și de stocare, principiul reducerii la minimum a datelor, exactitatea, integritatea și confidențialitatea datelor cu caracter personal, păstrând documente care să ateste respectarea obligațiilor sale.

Ori de câte ori constatăm că prelucrarea datelor cu caracter personal poate avea ca temei legal doar consimțământul, este de recomandat parcurgerea următoarelor etape, ca să ne asigurăm conformitatea cu cerințele Regulamentului european, respectiv:

1. verificăm dacă consimțământul este cel mai adecvat temei legal pentru prelucrare;
2. cererea consimțământului pentru prelucrare este separată de alți termeni și alte condiții;
3. cerem persoanelor vizate să ne dea consimțământul prin metode opt-in;
4. nu folosim căsuțe prebifate sau orice alt tip de consimțământ implicit;
5. limbajul folosit este unul simplu, ușor de înțeles;
6. menționăm de ce colectăm datele cu caracter personal și ce facem cu ele;
7. solicităm consimțământ distinct pentru fiecare scop în parte;
8. în interiorul notificării, am denumit organizația noastră și terțe persoane care vor avea acces la date;
9. am explicat că persoana vizată are dreptul să își retragă consimțământul;
10. asigurăm că retragerea consimțământului poate fi făcută fără vreun prejudiciu;
11. serviciul nostru nu este condiționat de consimțământ;
12. dacă oferim servicii minorilor, asigurăm metode prin care verificăm vârsta persoanelor vizate și obținem acordul părinților/reprezentanților.

[60] Art. 5 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).