editorial

Integrarea dreptului cu tehnologia în era digitală

The integration of law with technology in the digital age

DORU DOROBANŢU*

Putem astăzi spune, fără a greşi, că recenta criză pandemica COVID-19 a fost de natură a conduce la intensificarea extremă, în toată lumea, a aşa-numitul fenomen de transformare digitală şi a efectelor acestuia.

Urmare a măsurilor fără precedent generate de pandemie, copii şi adulţi am fost cu toţii „împinşi" către mediile virtuale, iar aceste schimbări de amploare se află la originea unor efecte multiple de durată, chiar dacă situaţia socio-economică a revenit oarecum la normal.

În perioada aceasta, am fost martorii adoptării în multe domenii a unor soluţii, instrumente şi servicii bazate pe tehnologie şi internet care au accelerat tranziţia noastră, a tuturor, către ceea ce numim economie digitală. Desigur, suntem conştienţi că toate acestea au necesitat şi vor necesita şi în continuare utilizarea pe scară largă a unui volum şi a unor categorii extinse de date, inclusiv date din categoria celor cu caracter personal.

Având în vedere acest context, dar şi evoluţiile fireşti preconizate ale noilor tehnologii ce presupun interferenţa tot mai mare cu inteligenţa artificială (IA)[1] pentru viitorul nostru, a devenit cu atât mai important ca protecţia datelor cu caracter personal să devină un pilon central al educaţiei juridice chiar de la cele mai fragede vârste.

Este necesar să anticipăm şi să planificăm pe termen mediu şi lung, să identificăm principiile şi măsurile ce ar putea conduce la dezvoltarea unui nou model eficient de educaţie privind protecţia datelor pentru fiecare nivel, de la copil la adult, de la şcolar la student şi tot aşa, care să integreze dinamic o înţelegere aprofundată a drepturilor şi libertăţilor fundamentale, a noilor tehnologii inovative, dar şi a designului juridic ce poate pune laolaltă în mod echitabil aceste lucruri.

Vom putea oferi astfel generaţiilor prezente şi viitoare oportunitatea de a construi şi înţelege, dintr-o perspectivă interdisciplinară, pe baza cunoştinţelor dobândite, modul în care reglementări juridice privind protecţia unor drepturi fundamentale pot opera şi

* Cadru didactic asociat la Universitatea Politehnica din Bucureşti.

[1] https://ro.wikipedia.org/wiki/Inteligen%C8%9B%C4%83_artificial%C4%83.

interacţiona, în viaţa de zi cu zi, cu produse, tehnologii şi servicii inovatoare de care, desigur, societatea are nevoie.

Realitate evidentă a zilelor noastre, inteligenţa artificială a devenit de ceva timp un instrument fără de care nu mai concepem interacţiunea şi evoluţia societăţii noastre. Identificată în strategia UE ca una dintre cele mai relevante tehnologii ale secolului 21 şi de maximă importanţă pentru transformarea digitală, IA poate contribui decisiv în arii diferite ale societăţii, precum analiza datelor şi automatizarea proceselor, tratamentul bolilor cronice, lupta împotriva schimbărilor climatice sau anticiparea ameninţărilor cybersecurity.

Computerele şi maşinile virtuale învaţă datorită algoritmilor complecşi care le permit să analizeze seturi uriaşe de date şi să facă predicţii folosind aceste date. În acelaşi timp, odată cu îmbunătăţirea abilităţilor maşinilor, sunt colectate cantităţi tot mai mari de date şi sunt monitorizate informaţii sensibile privind comportamentul uman, iar toate acestea prezintă provocări serioase pentru confidenţialitate şi protecţia datelor sau alte drepturi fundamentale.

Este din ce în ce mai evident că viitoare reglementări privind protecţia datelor vor trebui să fie mult mai adânc încorporate în arhitectura noilor tehnologii şi a proceselor decizionale automate, urmând abordarea confidenţialităţii *by design* şi *by default,* astfel încât să facă faţă complexului proces de transformare digitală şi efectelor sociale asociate cu proliferarea noilor tehnologii.

Identificăm astfel în mediul juridic, dar şi la nivel general, o nevoie rezonabilă a unei înţelegeri tehnice mult mai bună a noilor tehnologiilor care ne înconjoară, a reţelelor de comunicaţii şi a evoluţiei tehnologiilor digitale, cum ar fi inteligenţa artificială. Totodată, trebuie să identificăm şi alte abilităţi şi capacităţi specifice unui subiect care sunt importante într-o lume aflată într-o continuă schimbare.

În considerarea celor de mai sus, juriştii specialişti în protecţia datelor vor trebui să fie în măsură a-şi asuma rolul de participanţi activi în echipe multidisciplinare de specialişti care vor colabora la proiectarea de noi soluţii pentru problemele viitorului. Abilitatea de a lucra cu, şi de a media între parteneri de proiect specializaţi în noile tehnologii este şi va fi din ce în ce mai necesară. În funcţie de specificul proiectelor, în lumea digitală, juriştii specializaţi în protecţia datelor vor trebui să lucreze mult mai strâns cu inginerii de software, dezvoltatorii, designerii şi alţi experţi şi specialişti tehnici.

În acest sens, trebuie să fie capabili să înţeleagă nu numai problemele tehnice şi juridice implicate, ci şi interacţiunile „om-maşină" aferente unor procese, precum şi interfeţele dintre diferitele părţi interesate şi sistemele complexe controlate de noile tehnologii.

Un studiu recent al Agenţiei Uniunii Europene pentru Drepturile Fundamentale (EU Agency for Fundamental Rights – FRA)[2] privind algoritmii utilizaţi de tehnologiile IA demonstrează cum viaţa noastră privată şi anumite drepturi pot fi afectate de anumiţi algoritmi utilizaţi pentru identificarea prejudecăţilor, în aşa fel încât se poate ajunge la discriminare pe criterii religioase, de gen, sau de apartenenţă la o anumită minoritate etnică.

Este doar un exemplu, ceea ce nu înseamnă că trebuie să desfiinţăm sau să încetăm investiţiile în inteligenţa artificială sau utilizarea pe scară largă a noilor tehnologii.

Trebuie să înţelegem însă că factorul uman are un rol deosebit de important de jucat în integrarea dreptului cu noile tehnologii, că trebuie să avem o abordare orientată spre protecţia drepturilor fundamentale care să cultive capacităţi şi abilităţi semnificative mult mai strâns aliniate cu nevoile şi valorile erei digitale.

[2] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf.

Protecţia juridică a imaginii video a persoanei fizice. Soluţii practice şi jurisprudenţiale

Legal protection of the video images of the natural person. Practical and jurisprudential solutions

CARMEN TODICĂ*

❑ Rezumat

Fără a epuiza categoria largă a obligaţiilor operatorilor de date cu caracter personal, studiul îşi propune o incursiune asupra principalelor dispoziţii legale conţinute de Regulamentul general privind protecţia datelor şi legislaţia internă conexă, Ghidul nr. 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video, precum şi a dispoziţiilor Codului civil privind temeiul legal al despăgubirilor acordate. Studiul tratează probleme de interes practic privind informarea şi drepturile persoanelor vizate, temeiul legal al prelucrării imaginii persoanei fizice, inclusiv a pacientului şi salariaţilor, drepturile persoanei vizate şi plata de despăgubiri în caz de prelucrarea ilegală a imaginii persoanei, cu o trecere în revistă a sancţiunilor aplicate în domeniul analizat de către ANSPDCP.

Cuvinte-cheie: *prelucrare, imagine video, despăgubiri, informare, temei legal, consimţământ, persoană vizată.*

❑ Abstract

Without exhausting the wide category of obligations of personal data controllers, the study aims at a foray into the main legal provisions contained in the General Data Protection Regulation and the related national legislation, Guide no. 3/2019 on the processing of personal data by video means, as well as the provisions of the Civil Code on the legal basis of the compensations awarded. The study deals with issues of practical interest regarding the information and the rights of the data subjects, the legal basis for the processing of the image of the natural person, including the patient and employees, the rights of the data subject and the payment of damages in case of illegal processing of the person's image, with a review of the sanctions applied in the field analyzed by the ANSPDCP.

* Conf. univ. dr., vicepreşedinte Curtea de Arbitraj Bucureşti de pe lângă Camera de Comerţ şi Industrie Bucureşti, formator I.N.P.P.A., formator responsabil protecţia datelor, avocat asociat S.C.A. Marina & asociaţii.

***Keywords**: processing, video image, compensation, information, legal basis, consent, data subject.*

Preambul

Monitorizarea video a persoanei a devenit o uzanţă şi o permanenţă a zilelor noastre. Deşi utilizată în scopuri de protecţie a proprietăţii sau pentru a proteja viaţa şi sănătatea persoanei, această activitate presupune culegerea şi păstrarea de imagini vizuale ale persoanelor care intră în spaţiul monitorizat. Aceste persoane pot fi identificate în funcţie de aspect sau de alte elemente specifice, ceea ce face ca „indirect", monitorizarea video să fie percepută ca o intruziune în viaţa privată a persoanei.

Tocmai pentru a respecta această limită între interesul operatorului de a monitoriza video persoana vizată şi drepturile şi libertăţile acesteia, Regulamentul general privind protecţia datelor[1] şi legislaţia conexă impun operatorilor de date respectarea unor obligaţii. Departe de a epuiza în integralitatea lor obligaţiile operatorilor, în studiul de faţă ne vom apleca asupra unor aspecte controversate în practica protecţiei datelor cu caracter personal.

1. Stabilirea scopurilor prelucrării

O primă obligaţie a operatorului de date vizează stabilirea scopurilor prelucrării. Supravegherea video poate servi mai multor scopuri, de exemplu asigurarea protejării proprietăţii şi a altor bunuri, asigurarea protejării vieţii şi a integrităţii fizice a persoanelor. Scopurile monitorizării trebuie să fie specificate în detaliu şi documentate în scris. Supravegherea video având ca scop doar „siguranţa" sau „pentru siguranţa dumneavoastră" nu este suficient de specifică. În plus, persoanele vizate trebuie să fie informate cu privire la scopul (scopurile) prelucrării, iar odată stabilite, prelucrarea nu trebuie deturnată de la scopul iniţial, de exemplu, nu se poate utiliza imaginea video a salariatului într-o cercetare disciplinară ulterioară.

Trebuie precizat însă că Regulamentul nu se aplică prelucrării datelor care nu fac nicio referire la o persoană (când persoana nu poate fi identificată, direct sau indirect). Astfel, nu constituie o prelucrare de date sub incidenţa Regulamentului, prelucrarea efectuată de o cameră video încorporată într-o maşină pentru a oferi asistenţă la parcare, reglată astfel încât să nu culeagă informaţii despre o persoană fizică, şi nici prelucrarea datelor cu caracter personal de către o persoană fizică în cadrul unei activităţi exclusiv personale sau domestice (în cadrul vieţii private sau de familie a persoanelor).

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

2. Informarea persoanei vizate

Înainte de prelucrarea imaginii video, operatorul trebuie să informeze persoana vizată[2]. Simpla pictogramă nu constituie o informare conformă cu Regulamentul. În acest sens, persoanele vizate trebuie să fie informate cu privire la scopul (scopurile) prelucrării în conformitate cu art. 13 din Regulament[3]. Ghidul nr. 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video[4] distinge între două tipuri de informări: semnul de avertizare (primul nivel) și un al doilea nivel cu informații detaliate.

[2] A patra sancțiune (disponibilă pe site-ul oficial www.dataprotection.ro) a fost acordată în luna iulie 2019 de Autoritatea Națională de Supraveghere (amendă în cuantum total de 11.834,25 lei, echivalentul sumei de 2.500 euro). Operatorul U.I. SRL nu a putut face dovada realizării informării persoanelor vizate cu privire la prelucrarea datelor cu caracter personal/imagini prin intermediul sistemului de supraveghere video, pe care o realiza începând din anul 2016. Într-o speță similară, Autoritatea Națională de Supraveghere a finalizat în data de 29 noiembrie 2019 o investigație la o Asociație de Proprietari și a constatat încălcarea anumitor dispoziții din Regulamentul General privind Protecția Datelor, aplicând sancțiunea amenzii (în cuantum de 2.389,05 lei, echivalentul a 500 euro) și măsura corectivă de a asigura conformitatea cu RGPD a operațiunilor de prelucrare efectuate prin intermediul sistemului de supraveghere video în sensul informării persoanelor vizate conform art. 12 și 13 din RGPD, inclusiv prin postarea unor avertizări și note de informare în apropierea locurilor unde sunt montate camerele video.

[3] Potrivit art. 13 alin. (1) din Regulament, *„În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, operatorul, în momentul obținerii acestor date cu caracter personal, furnizează persoanei vizate toate informațiile următoare: a)identitatea și datele de contact ale operatorului și, după caz, ale reprezentantului acestuia; b)datele de contact ale responsabilului cu protecția datelor, după caz; c)scopurile în care sunt prelucrate datele cu caracter personal, precum și temeiul juridic al prelucrării; d)în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f), interesele legitime urmărite de operator sau de o parte terță; e)destinatarii sau categoriile de destinatari ai datelor cu caracter personal; f)dacă este cazul, intenția operatorului de a transfera date cu caracter personal către o țară terță sau o organizație internațională și existența sau absența unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menționate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf, o trimitere la garanțiile adecvate sau corespunzătoare și la mijloacele de a obține o copie a acestora, în cazul în care acestea au fost puse la dispoziție. (2)În plus față de informațiile menționate la alineatul (1), în momentul în care datele cu caracter personal sunt obținute, operatorul furnizează persoanei vizate următoarele informații suplimentare necesare pentru a asigura o prelucrare echitabilă și transparentă: a)perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă; b)existența dreptului de a solicita operatorului, în ceea ce privește datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ștergerea acestora sau restricționarea prelucrării sau a dreptului de a se opune prelucrării, precum și a dreptului la portabilitatea datelor; c)atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a), existența dreptului de a retrage consimțământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimțământului înainte de retragerea acestuia; d)dreptul de a depune o plângere în fața unei autorități de supraveghere; e)dacă furnizarea de date cu caracter personal reprezintă o obligație legală sau contractuală sau o obligație necesară pentru încheierea unui contract, precum și dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal și care sunt eventualele consecințe ale nerespectării acestei obligații; f)existența unui proces decizional automatizat incluzând crearea de profiluri".*

[4] Versiunea 2.0., adoptat la 29 ianuarie 2020.

Semnul de avertizare (primul nivel) cuprinde o pictogramă în combinaţie cu scopurile prelucrării, identitatea operatorului şi existenţa drepturilor persoanei vizate. Acesta trebuie poziţionat astfel încât persoana vizată să poată recunoaşte cu uşurinţă circumstanţele supravegherii înainte de a intra în zona monitorizată (aproximativ la nivelul ochilor). Nu este necesar să se divulge poziţia camerei, atâta timp cât nu există niciun dubiu asupra zonelor supuse monitorizării (pct. 112 şi 113 din Ghid).

Detalii obligatorii prevăzute de art. 13 din Regulament vor fi furnizate prin alte mijloace (al doilea nivel). Informaţiile din cel de-al doilea nivel trebuie să poată fi accesate de către persoana vizată fără a intra în zona supravegheată. Pentru acest motiv, sugerăm postarea informării din cel de al doilea nivel la intrarea în incinta operatorului, dar şi pe site-ul acestuia. Suplimentar, recomandăm, afişarea informării într-un loc uşor accesibil, de exemplu sub forma unei fişe cu informaţii complete, disponibilă într-un loc central (de exemplu, birou de informaţii, recepţie sau casierie) sau afişate pe un panou uşor accesibil (pct. 117 din Ghid). În mod obligatoriu, informarea va cuprinde temeiurile prelucrării imaginii video de către operator.

3. Temeiurile prelucrării imaginii video

Oricare dintre temeiurile juridice prevăzute la art. 6 alin. (1) din Regulament poate constitui un temei juridic pentru prelucrarea imaginii video. Cu toate aceste, în practică, cele mai frecvente temeiuri legale pe care un operator îşi fundamentează prelucrarea este interesul legitim [art. 6 alin. (1) lit. (f) din Regulament] şi necesitatea de a îndeplini o sarcină care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice [art. 6 alin. (1) lit. (e)]. Apreciem că doar în mod excepţional, operatorul ar putea utiliza ca temei juridic consimţământul persoanei vizate [art. 6 alin. (1) lit. (a)].

3.1. Interesul legitim urmărit de operator[5]. Potrivit art. 6 alin. (1) lit. (f) din Regulament, supravegherea video este legală dacă este necesară pentru a îndeplini scopul unui interes legitim urmărit de un operator sau de o parte terţă, cu excepţia cazului în care interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate prevalează asupra acestor interese. Astfel, ori de câte ori prelucrarea imaginii video se fundamentează pe interesul legitim urmărit de operator, acesta trebuie să dovedească şi să documenteze temeinic motivul prelucrării. Interesul legitim trebuie să existe şi să fie actual (adică nu trebuie să fie fictiv sau speculativ)[6].

În practică sunt apreciate ca fiind situaţii ce fundamentează interesul legitim urmărit de operator „paza şi protecţia bunurilor şi persoanelor". Cu toate acestea, interesul legitim nu poate fi invocat în mod arbitrar şi nu poate justifica orice instalare a unei camere video, fiind obligatorie o evaluare comparativă a intereselor. Astfel, un sistem de supraveghere video poate fi pus în funcţiune după ce în prealabil operatorul a efectuat un test comparativ între interesele legitime urmărite şi drepturile şi libertăţile fundamentale ale persoanei vizate. În efectuarea testului comparativ, operatorul trebuie

[5] Interesele legitime urmărite de un operator pot fi interese juridice (Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-13/16, *Rīgas satiksme*, 4 mai 2017), economice sau morale (Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video, p. 10).

[6] Cauza CJUE C-708/18, p. 44.

să ia în considerare, pe de o parte, în ce măsură monitorizarea afectează interesele, drepturile şi libertăţile fundamentale ale persoanelor, iar pe de altă aparte, dacă acest lucru provoacă încălcări ale drepturilor persoanei vizate sau consecinţe negative cu privire la acestea. Dacă interesele sau drepturile şi libertăţile fundamentale ale persoanei vizate prevalează asupra intereselor legitime ale operatorului, sistemul de supraveghere video nu trebuie instalat. În practică, testul comparativ a demonstrat riscuri maxime de intruziune asupra drepturilor persoanei vizate prin instalarea camerelor de luat vederi în zone precum: grupurile sanitare sau saună, zonele destinate servirii mesei angajaţilor.

În acest sens, Autoritatea Naţională de Supraveghere a sancţionat activitatea de prelucrare a imaginii angajaţilor de către operator în mod excesiv, prin intermediul camerelor video instalate în spaţii cu destinaţia de vestiare şi în zona destinată servirii mesei, invocând scopul protejării bunurilor şi a produselor societăţii, precum şi al descurajării furtului[7].

Tot astfel, spaţiile folosite în mod obişnuit pentru activităţi de recuperare, regenerare şi recreere[8], sălile de tratament şi de consultaţie a unui pacient constituie zone cu risc de intruziune intensă asupra drepturilor persoanei vizate.

3.2. Îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul. Potrivit art. 6 alin. (1) teza 2 din Regulament, autorităţile publice nu pot prelucra datele cu caracter personal în temeiul interesului legitim atât timp cât se află în îndeplinirea atribuţiilor lor. Pentru acest motiv, temeiul juridic care justifică monitorizare video a spaţiilor din instituţii publice rămâne îndeplinirea unei sarcinii care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul.

Cu privire la acest temei legal, art. 6 din Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului[9] instituie cerinţe suplimentare în ipoteza în care prelucrarea datelor personale şi speciale este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public, deci inclusiv în cazul instalării sistemelor de monitorizare video. În acest caz, operatorul instituţie sau autoritate publică este obligat să pună

[7] A se vedea Decizia de sancţionare a ANSPDCP din 15 aprilie 2021, disponibilă pe site-ul oficial www.dataprotection.ro. Operatorul a fost sancţionat contravenţional cu amendă în cuantum de 24.362,50 lei (echivalentul în lei al sumei de 5.000 Euro). Autoritatea Naţională de Supraveghere a apreciat că scopul declarat de operator (protejarea bunurilor, a produselor societăţii şi descurajarea furtului) se putea realiza prin mijloace mai puţin intruzive pentru viaţa privată a angajaţilor. Operatorului respectiv i-au fost aplicate şi o serie de măsuri corective, printre care să reanalizeze orientarea unghiului de captare a imaginilor video astfel încât să nu monitorizeze activitatea angajaţilor săi în spaţii cu destinaţia de vestiare şi în sala de mese, raportat la scopul prelucrării.

[8] Ghidul include şi locurile în care persoanele stau şi/sau comunică, de exemplu în zone de odihnă, la mese de restaurant, în parcuri, la cinematografe şi în centre de fitness, apreciind că şi în aceste situaţii, interesele sau drepturile şi libertăţile persoanei vizate vor prevala deseori asupra intereselor legitime ale operatorului (pct. 38 din Ghid).

[9] Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului UE 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (publicată în M. Of. nr. 651 din 26 iulie 2018), astfel cum a fost modificată şi completată ulterior, prin Legea nr. 233 din 27 noiembrie 2019 (M. Of. nr. 956 din 28 noiembrie 2019).

în aplicare măsurile tehnice şi organizatorice adecvate pentru respectarea principiilor enumerate de art. 5[10] din Regulament în special cel a reducerii la minimum a datelor, principiul integrităţii şi confidenţialităţii, să desemneze un responsabil pentru protecţia datelor, să stabilească termene de stocare în funcţie de natura datelor şi scopul prelucrării, precum şi de termene specifice în care datele cu caracter personal trebuie şterse sau revizuite în vederea ştergerii.

Un caz particular în care a fost invocat ca temei exercitarea autorităţii publice cu care este învestit operatorul, l-a constituit monitorizarea persoanelor vizate de către Poliţia locală, prin sisteme body cam. Deşi în aparenţă temeiul legal era suficient pentru a justifica o atare prelucrare, opinia ANSPDCP a fost diametral opusă, sancţionând astfel de prelucrări.

În anul 2020 o unitate teritorial administrativă a fost sancţionată contravenţional cu avertisment, întrucât personalul Direcţiei Generale de Poliţie Locală, aflat în exercitarea misiunilor şi activităţilor specifice, a prelucrat date cu caracter personal prin utilizarea sistemului audio-video portabil de tip „Body-Worn Camera" (care prelucrează imaginea şi vocea), începând cu luna octombrie 2019, fără să existe o obligaţie legală a operatorului şi fără îndeplinirea vreunei alte condiţii prevăzute la art. 6 alin. (1) din Regulament[11].

---

[10] Potrivit art. 5 din Regulament „Principii legate de prelucrarea datelor cu caracter personal (1) Datele cu caracter personal sunt: a) prelucrate în mod legal, echitabil şi transparent faţă de persoana vizată («legalitate, echitate şi transparenţă»); b) colectate în scopuri determinate, explicite şi legitime, şi nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile iniţiale, în conformitate cu articolul 89 alineatul (1) («limitări legate de scop»); c) adecvate, relevante şi limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate («reducerea la minimum a datelor»); d) exacte şi, în cazul în care este necesar, să fie actualizate; trebuie să se ia toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt şterse sau rectificate fără întârziere («exactitate»); e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depăşeşte perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare ştiinţifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), sub rezerva punerii în aplicare a măsurilor de ordin tehnic şi organizatoric adecvate prevăzute în prezentul regulament în vederea garantării drepturilor şi libertăţilor persoanei vizate («limitări legate de stocare»); f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecţia împotriva prelucrării neautorizate sau ilegale şi împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare («integritate şi confidenţialitate»)".

[11] Disponibilă pe pagina oficială www.dataprotetion.ro. Investigaţia a fost efectuată ca urmare a primirii unei sesizări cu privire la încălcarea legislaţiei privind protecţia datelor cu caracter personal de către Direcţia Generală de Poliţie Locală.

S-a constatat că Direcţia Generală de Poliţie prelucrează date cu caracter personal prin intermediul sistemelor audio-video portabile de tip „Body-Worn Camera", utilizate de către poliţiştii locali aflaţi în exercitarea atribuţiilor de serviciu pentru înregistrarea următoarelor categorii de intervenţii şi acţiuni:

a) legitimarea persoanelor;

b) conducerea persoanelor la sediul poliţiei locale;

c) utilizarea forţei şi a mijloacelor din dotare;

Într-un caz similar, în data de 11 decembrie 2020 o altă unitate administrativ teritorială a fost sancţionată contravenţional cu avertisment, însoţit de măsură corectivă, dispusă prin planul de remediere, de a asigura conformitatea operaţiunilor de prelucrare, efectuate prin utilizarea mijloacelor de supraveghere audio-video de tip „BADGE", cu dispoziţiile art. 5 şi art. 6 din RGPD. Investigaţia a fost demarată în urma primirii unei sesizări cu privire la încălcarea legislaţiei privind protecţia datelor şi s-a constatat că Direcţia Generală de Poliţie Locală prelucrează date cu caracter personal prin intermediul unor mijloace de supraveghere audio-video portabile, de tip „BADGE", utilizate de către personalul Direcţiei în misiuni şi activităţi derulate pe teren, în contextul în care poliţiştilor locali le-a fost stabilită ierarhic obligaţia de a purta asupra lor, în timpul programului de lucru aceste mijloace de supraveghere audio-video.

În motivarea aplicării sancţiunilor, Autoritate a constatat că nu există dispoziţii legale care să reglementeze utilizarea unor sisteme de supraveghere audio-video portabile în activitatea poliţiştilor locali. Ca atare, s-a constatat că prelucrarea datelor cu caracter personal (imagine, voce) s-a efectuat fără îndeplinirea condiţiilor de legalitate a prelucrării, aşa cum sunt prevăzute în art. 6 alin. (1) din RGPD.

În raport de acesta concluzie, se ridică întrebarea de ce *îndeplinirea unei sarcini care serveşte unui interes public sau care rezultă din exercitarea autorităţii publice cu care este învestit operatorul* nu este un temei necesar şi suficient pentru a justifica o atare prelucrare?

Răspunsul se regăseşte în considerentul nr. 45 din Regulament potrivit căruia „*În cazul în care prelucrarea este efectuată în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existenţa unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operaţiuni de prelucrare efectuate în conformitate cu o obligaţie legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care serveşte unui interes public sau care face parte din exercitarea autorităţii publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condiţiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificaţiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităţilor cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcţie de scop, a perioadei de stocare şi a altor măsuri pentru a garanta o prelucrare legală şi echitabilă".*

---

d) efectuarea controlului corporal sau al bagajului;

e) oprirea vehiculelor;

f) constatarea infracţiunilor flagrante şi a contravenţiilor;

g) cele determinate de prevenirea unui pericol iminent la adresa vieţii, sănătăţii şi integrităţii fizice a unei persoane.

Direcția Generală de Poliție Locală nu a putut face dovada respectării art. 6 alin. (1) din RGPD privind legalitatea prelucrării efectuate prin intermediul sistemului audio-video portabil de tip „Body-Worn Camera". În consecință, s-a constatat că prelucrarea datelor cu caracter personal (imagine, voce) s-a efectuat fără îndeplinirea condițiilor de legalitate prevăzute la art. 6 alin. (1) din RGPD.

Prin urmare temeiul *îndeplinirii unei sarcini care servește unui interes public sau exercitarea autorității publice* nu este justificat cât timp nu este dublat de o măsura legislativă, un act normativ care să stabilească cel puțin scopul prelucrării, specificațiile pentru stabilirea operatorului îndreptățit la o astfel de prelucrare, tipului de date cu caracter personal care fac obiectul prelucrării, persoane vizate, entitățile cărora le pot fi divulgate datele cu caracter personal, limitările în funcție de scop, perioada de stocare. În lipsa unei măsuri legislative care să autorizeze fundamentarea pe temeiul interesului public sau exercitării autorității publice, prelucrarea nu este **legală și echitabilă.**

3.3. Consimțământul persoanei vizate. Monitorizarea video implică prin natura tehnologiei captarea și prelucrarea imaginii unui număr necunoscut de persoane. În acest context, poate fi dificil pentru un operator să demonstreze că persoana vizată și-a dat consimțământul înainte de prelucrarea datelor sale personale, în conformitate cu art. 7 alin. (1) din Regulament. Totodată, în măsura în care persoana vizată își retrage consimțământul, va fi dificil pentru operator să demonstreze că datele cu caracter personal nu mai sunt prelucrate. În acest context, Ghidul recomandă la pct. 43 ca în ceea ce privește monitorizarea sistematică, consimțământul persoanei vizate nu poate servi ca temei juridic decât în cazuri excepționale. Cu alte cuvinte, un operator va apela la consimțământul persoanei vizate doar în condițiile în care nu există alt temei legal pentru a justifica prelucrarea video. Suplimentar, operatorul este obligat să facă dovada consimțământului persoanei vizate[12], respectiv să se asigure că orice persoană vizată care intră în zona aflată sub supraveghere video și-a dat consimțământul. În ipoteza imposibilității obținerii unui formular scris de consimțământ al persoanei vizate, apreciem că este posibil un consimțământ exprimat verbal, cu condiția ca operatorul să fie în măsură să demonstreze că persoana vizată și-a dat acordul pentru prelucrarea datelor sale cu caracter personal.

O problemă care a suscitat interesul practicii de specialitate în domeniul protecție datelor cu caracter personal, a fost întrebarea dacă se solicită sau nu consimțământul salariaților pentru monitorizarea video. De cele mai multe ori, în practică, pentru a asigura o dovadă reală, operatorul solicită un consimțământ expres al angajaților în acest.

Având în vedere raportul de subordonare în executarea contractului de muncă dintre angajatori și angajați, un atare consimțământ nu poate fi calificat ca „fiind liber acordat" și din această perspectivă consimțământul este viciat, neproducând efecte juridice. În acest context, operatorul nu ar trebui să se bazeze pe consimțământ atunci când prelucrează date cu caracter personal al salariaților, nici în ceea ce privește prelucrarea imaginii video.

Anterior Regulamentului, soluția era oferită de prevederile Avizului nr. 2/2017 privind prelucrarea datelor la locul de muncă din 8 iunie 2017 *„pentru cea mai mare parte a acțiunii de prelucrare a datelor cu caracter personal la locul de muncă, temeiul juridic nu poate și nu ar trebui să fie consimțământul angajaților, având în vedere natura relației dintre angajator și angajat"*. În contextul apariției Regulamentului, Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video elucidează problema, recomandând: *„Având în vedere dezechilibrul de putere dintre angajatori și angajați, în majoritatea cazurilor, angajatorii nu trebuie să se bazeze pe consimțământ*

[12] Consimțământul trebuie să fie acordat în mod liber, specific, în cunoștință de cauză și lipsit de ambiguitate (Ghid privind consimțământul conform Regulamentului 2016/679 (WP 259 rev. 01) – aprobat de CEPD).

atunci când prelucrează date cu caracter personal, deoarece este puțin probabil ca acesta să fie acordat în mod liber" (pct. nr. 47 din Ghid)[13].

Mai elocventă în acest sens este practica ANSPDCP care, în Deciziile de sancționare a operatorilor, a formulat și recomandări și argumente juridice. Astfel, în investigațiile desfășurate, raportat la aspectul analizat (consimțământul salariaților), ANSPDCP a reținut: „*având în vedere relația angajator-angajat, nu a putut fi considerat liber exprimat consimțământul persoanei vizate și nici nu a putut fi identificat alt temei legal de prelucrare, operatorul neputând face dovada respectării principiilor de prelucrare, prin raportare și la art. 5 alin. (2) din Regulamentul General privind Protecția Datelor*"[14].

Într-o speță similară[15] ANSPDCP oferă și soluția: „*în măsura în care un angajator utilizează sisteme de monitorizare prin mijloace de supraveghere video la locul de muncă, prelucrarea datelor cu caracter personal ale angajaților în scopul realizării intereselor legitime ale angajatorului [art. 6 alin. (1) lit. f) din RGPD] se realizează cu respectarea dispozițiilor art. 5 din Legea nr. 190/2018 care stabilesc, ca primă condiție, pe aceea ca interesele legitime urmărite de angajator să fie temeinic justificate și să prevaleze asupra intereselor sau drepturilor și libertăților persoanelor vizate*".

În completarea Regulamentului, Legea nr. 190/2018 stabilește condiții suplimentare pentru monitorizarea salariaților prin mijloace de supraveghere video la locul de muncă. Art. 5 din Legea nr. 190/2018, intitulat sugestiv „Prelucrarea datelor cu caracter personal în contextul relațiilor de muncă", prevede condițiile pentru utilizarea mijloace de supraveghere video: „*prelucrarea datelor cu caracter personal ale angajaților, în scopul realizării intereselor legitime urmărite de angajator, este permisă numai dacă: a) interesele legitime urmărite de angajator sunt temeinic justificate și prevalează asupra intereselor sau drepturilor și libertăților persoanelor vizate (efectuarea testului comparativ); b) angajatorul a realizat informarea prealabilă obligatorie, completă și în mod explicit a angajaților (informarea salariaților potrivit art. 13 din Regulament); 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 (angajatorul să dovedească că alte măsuri nu au fost eficiente), 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*".

Suplimentar acestor cerințe, operatorul trebuie să efectueze și o evaluare a impactului asupra protecției datelor[16] (D.P.I.A.).

---

[13] http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

[14] Decizia de sancționare a operatorul SC T.T.F.I. SRL cu amendă în cuantum de 24.362,50 lei (echivalentul în lei al sumei de 5.000 Euro).

[15] În data de 23 septembrie 2021, operatorul G.T. SRL este sancționat contravențional **cu amendă în cuantum de 24.745,00 lei (echivalentul a 5.000 EURO).** S-a constatat faptul că operatorul a prelucrat date cu caracter personal ale angajaților săi prin utilizarea unui sistem audio-video (imagine și voce), fără a face dovada respectării temeiurilor legale prevăzute de art. 6 alin. (1) din RGPD. Investigația a fost demarată ca urmare a unei sesizări, prin care se semnala faptul că operatorul G.T. SRL avea instalate unele camere de supraveghere audio-video în interiorul birourilor, pentru supravegherea directă a angajaților la locul de muncă unde își desfășoară activitatea și înregistrarea discuțiilor dintre aceștia, în scopul utilizării lor ulterioare împotriva respectivilor angajați.

[16] A se vedea infra pct. 4. Autoritatea Națională de Supraveghere a finalizat, pe data de 13 decembrie 2019, o investigație la operatorul E.S.T. SRL, acesta fiind sancționat, printre altele și cu