Ghidul 3/2019 privind prelucrarea datelor cu caracter personal prin mijloace video

Versiunea 2.0

Adoptat la 29 ianuarie 2020

Istoricul versiunilor

Versiunea 2.1	26 februarie 2020	Modificarea unei erori materiale
Versiunea 2.0	29 ianuarie 2020	Adoptarea ghidului în urma consultării publice
Versiunea 1.0	10 iulie 2019	Adoptarea ghidului pentru consultare publică

Cuprins

Comitetul European pentru Protecția Datelor,

având în vedere articolul 70 alineatul (1) litera (e) din 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 (denumit în continuare „RGPD”),

având în vedere Acordul privind SEE, în special anexa XI și Protocolul 37 la acesta, astfel cum au fost modificate prin Decizia nr. 154/2018 a Comitetului mixt al SEE din 6 iulie 2018[1],

având în vedere articolul 12 și articolul 22 din Regulamentul de Procedură al acestuia,

ADOPTĂ URMĂTORUL GHID

1 INTRODUCERE

1. Utilizarea intensivă a dispozitivelor video influențează comportamentul cetățenilor. Utilizarea pe scară largă a unor astfel de instrumente în multe domenii ale vieții persoanelor va face ca indivizii să simtă o presiune suplimentară de a preveni detectarea gesturilor care ar putea fi percepute ca anomalii. În fapt, aceste tehnologii pot restrânge posibilitățile de circulație anonimă și utilizare anonimă a serviciilor și, în general, limitează posibilitatea de a trece neobservat. Implicațiile pentru protecția datelor sunt enorme.

2. Chiar dacă persoanele fizice pot să nu fie deranjate de supravegherea video instituită pentru un anumit scop, de exemplu legat de securitate, trebuie luate măsuri pentru a asigura evitarea oricărei utilizări necorespunzătoare în scopuri total diferite și neașteptate pentru persoana vizată (de exemplu, scopuri de marketing, monitorizarea performanței angajaților etc.). În plus, în prezent se utilizează numeroase instrumente pentru exploatarea imaginilor captate și transformarea camerelor tradiționale în camere inteligente. Volumul de date generate de înregistrarea video, împreună cu aceste instrumente și tehnici, mărește riscurile de utilizare secundară (legată sau nu de scopul atribuit inițial sistemului) sau chiar riscurile de utilizare abuzivă. Principiile generale ale RGPD (articolul 5) ar trebui să fie atent luate în considerare de fiecare dată când se face referire la supravegherea video.

3. Sistemele de supraveghere video schimbă în multe feluri modul de interacțiune a profesioniștilor din sectorul privat și din sectorul public în locuri private sau publice, în scopuri de îmbunătățire a securității, de analizare a publicului, furnizare de publicitate personalizată etc. Supravegherea video a devenit deosebit de performantă prin utilizarea extinsă a analizei video inteligente. Aceste tehnici pot fi mai invazive (de exemplu, tehnologii biometrice complexe) sau mai puțin invazive (de exemplu, simpli algoritmi de numărare). Păstrarea anonimității și protejarea vieții private devin din ce în ce mai dificile în general. Problemele legate de protecția datelor pot fi

[1] Referirile la „statele membre” din acest aviz trebuie înțelese ca referiri la „statele membre ale SEE”.

diferite în funcție de situație; la fel și analiza juridică atunci când se utilizează una sau alta dintre aceste tehnologii.

4. Pe lângă aspectele de confidențialitate, există și riscuri legate de posibila funcționare defectuoasă a acestor dispozitive și de atitudinile părtinitoare pe care le pot induce. Cercetătorii semnalează că software-ul utilizat pentru identificare, recunoaștere sau analiză facială funcționează diferit în funcție de vârsta, genul și originea etnică a persoanei pe care o identifică. Algoritmii funcționează pe baze demografice diferite, astfel că lipsa obiectivității în recunoașterea facială amenință să consolideze prejudecățile societății. De aceea, operatorii de date trebuie să asigure și faptul că prelucrarea datelor biometrice care rezultă din supravegherea video face obiectul unei evaluări periodice a relevanței și a suficienței garanțiilor oferite.

5. Supravegherea video nu constituie o necesitate în mod implicit atunci când există și alte mijloace pentru atingerea scopului principal. Altfel, apare riscul de modificare a normelor culturale care ar duce la acceptarea lipsei de confidențialitate ca premisă generală.

6. Prezentul ghid își propune să furnizeze orientări cu privire la modul de aplicare a RGPD în legătură cu prelucrarea datelor cu caracter personal prin intermediul dispozitivelor video. Exemplele nu sunt exhaustive, raționamentul general putând fi aplicat tuturor domeniilor de utilizare potențiale.

2 SFERA DE APLICARE[2]

2.1 Datele cu caracter personal

7. Monitorizarea automatizată sistematică a unui spațiu specific prin mijloace optice sau audio-video, în principal în scopuri de protecție a proprietății sau pentru a proteja viața și sănătatea persoanei, a devenit un fenomen important al zilelor noastre. Această activitate presupune culegerea și păstrarea de informații sub formă de imagini sau informații audio-vizuale despre toate persoanele care intră în spațiul monitorizat, și care pot fi identificate în funcție de aspect sau de alte elemente specifice. Identitatea acestor persoane poate fi stabilită pe baza acestor detalii. De asemenea, este posibilă prelucrarea suplimentară a datelor cu caracter personal cu privire la prezența și comportamentul persoanelor în spațiul dat. Riscul potențial de utilizare abuzivă a acestor date crește în raport cu dimensiunea spațiului monitorizat, precum și cu numărul persoanelor care frecventează spațiul respectiv. Acest fapt este reflectat de Regulamentul general privind protecția datelor în articolul 35 alineatul (3) litera (c), care prevede efectuarea unei evaluări a impactului asupra protecției datelor în cazul unei monitorizări sistematice pe scară largă a unei zone accesibile publicului, precum și în articolul 37 alineatul (1) litera (b), care impune operatorilor să desemneze un responsabil cu protecția datelor, dacă operațiunea de prelucrare, prin natura sa, necesită o monitorizare periodică și sistematică a persoanelor vizate.

8. Totuși, regulamentul nu se aplică prelucrării datelor care nu fac nicio referire la o persoană, de exemplu atunci când persoana nu poate fi identificată, direct sau indirect.

> Exemplu: RGPD nu se aplică pentru camerele false (adică orice dispozitiv care nu funcționează ca o cameră de luat vederi și, prin urmare, nu prelucrează date cu caracter personal). *Cu toate acestea, în unele state membre, s-ar putea ca această situație să cadă sub incidența altor prevederi legislative.*
>
> Exemplu: Înregistrările de la mare altitudine se încadrează în sfera de aplicare a RGPD numai dacă, în circumstanțele respective, datele prelucrate pot fi legate de o anumită persoană.
>
> Exemplu: O cameră video este încorporată într-o mașină pentru a oferi asistență la parcare. În cazul în care camera este construită sau reglată astfel încât să nu culeagă informații despre o persoană fizică (cum ar fi numărul de înmatriculare sau informații care ar putea identifica trecătorii), nu se aplică RGPD.

9.

2.2 Aplicarea Directivei privind protecția datelor în contextul aplicării legii (DARL) [(UE) 2016/680]

10. În special prelucrarea datelor cu caracter personal de către autoritățile competente în scopul prevenirii, depistării, investigării sau urmăririi penale a infracțiunilor sau al executării pedepselor, inclusiv al protejării împotriva amenințărilor la adresa securității publice și al prevenirii acestora intră sub incidența Directivei (UE) 2016/680.

[2] Comitetul European pentru Protecția Datelor (CEPD) observă că, în cazurile în care RGPD permite acest lucru, s-ar putea aplica cerințele specifice din legislația națională.

2.3 Derogarea privind activitățile domestice

11. În temeiul articolului 2 alineatul (2) litera (c), prelucrarea datelor cu caracter personal de către o persoană fizică în cadrul unei activități exclusiv personale sau domestice, care poate include și o activitate online, nu intră sub incidența RGPD[3].

12. Această dispoziție - așa-numita derogare privind activitățile domestice - în contextul supravegherii video trebuie interpretată strict. Astfel, după cum a considerat Curtea de Justiție a Uniunii Europene, așa-numita „derogare privind activitățile domestice" trebuie „*interpretată ca referindu-se doar la activitățile care se desfășoară în cadrul vieții private sau de familie a persoanelor, ceea ce în mod evident nu este cazul prelucrării de date cu caracter personal care constă în publicarea pe internet, astfel încât aceste date să devină accesibile unui număr nedeterminat de persoane*"[4]. În plus, dacă un sistem de supraveghere video, în măsura în care implică înregistrarea continuă și stocarea de date cu caracter personal și acoperă, „*chiar și parțial, un spațiu public și este, ca atare, direcționat spre exterior din cadrul privat al persoanei care prelucrează datele în acest mod, aceasta nu poate fi considerată o activitate exclusiv personală sau domestică în sensul articolului 3 alineatul (2) a doua liniuță din Directiva 95/46"*[5].

13. În ceea ce privește dispozitivele video care funcționează în spațiile unei persoane private, acestea pot intra sub incidența derogării privind activitățile domestice. Acest lucru depinde de mai mulți factori, care trebuie luați în considerare în totalitate pentru a ajunge la o concluzie. Pe lângă elementele menționate mai sus, identificate de hotărârile CJUE, utilizatorul dispozitivului de supraveghere video la domiciliu trebuie să stabilească dacă are vreun fel de relație personală cu persoana vizată, dacă amploarea sau frecvența supravegherii sugerează vreun fel de activitate profesională din partea sa, precum și potențialul impact negativ al supravegherii asupra persoanelor vizate. Prezența oricăruia dintre elementele menționate nu înseamnă neapărat că prelucrarea este în afara sferei derogării privind activitățile domestice, dar că este necesară o evaluare generală pentru a stabili acest lucru.

[3] Vezi și Considerentul 18.

[4] Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-101/01, Bodil Lindqvist, 6 noiembrie 2003, punctul 47.

[5] Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-212/13, František Ryneš/Úřad pro ochranu osobních údajů, 11 decembrie 2014, punctul 33.

Exemplu: Un turist face înregistrări video atât cu telefonul mobil, cât și cu o cameră video pentru a-și documenta vacanța. El arată filmările prietenilor și familiei, dar nu le pune la dispoziția unui număr nedeterminat de persoane. Această situație ar intra sub incidența derogării privind activitățile domestice.

Exemplu: O biciclistă care coboară o pantă pe munte vrea să-și înregistreze coborârea cu o cameră de acțiune. Ea merge cu bicicleta într-o zonă izolată și intenționează să folosească înregistrările acasă, doar pentru propriul divertisment. Această situație ar intra sub incidența derogării privind activitățile domestice, chiar dacă într-o anumită măsură sunt prelucrate date cu caracter personal.

Exemplu: Cineva își monitorizează și înregistrează activitățile din grădina proprie. Proprietatea este împrejmuită și numai operatorul și familia sa intră în grădină în mod regulat. Aceasta ar intra sub incidența derogării privind activitățile domestice, cu condiția ca supravegherea video să nu se extindă nici măcar parțial la un spațiu public sau la o proprietate învecinată.

14.

3 LEGALITATEA PRELUCRĂRII

15. Înainte de utilizare, scopurile prelucrării trebuie să fie specificate în detaliu [articolul 5 alineatul (1) litera (b)]. Supravegherea video poate servi mai multor scopuri, de exemplu asigurarea protejării proprietății și a altor bunuri, asigurarea protejării vieții și a integrității fizice a persoanelor, colectarea de probe pentru acțiunile civile[6]. Scopurile monitorizării trebuie documentate în scris [articolul 5 alineatul (2)] și trebuie specificate pentru fiecare cameră de supraveghere care se utilizează. Camerele care sunt utilizate în același scop de un singur operator pot fi documentate împreună. În plus, persoanele vizate trebuie să fie informate cu privire la scopul (scopurile) prelucrării în conformitate cu articolul 13 (*vezi secțiunea 7, Obligații privind transparența și informarea*). Supravegherea video având ca scop doar „siguranța" sau „pentru siguranța dumneavoastră" nu este suficient de specifică [articolul 5 alineatul (1) litera (b)]. În plus, acest lucru contravine principiului potrivit căruia datele cu caracter personal trebuie prelucrate în mod legal, echitabil și transparent în raport cu persoana vizată [vezi articolul 5 alineatul (1) litera (a)].

16. În principiu, oricare dintre temeiurile juridice prevăzute la articolul 6 alineatul (1) poate constitui un temei juridic pentru prelucrarea datelor provenite din supravegherea video. De exemplu, articolul 6 alineatul (1) litera (c) se aplică în situațiile în care legislația națională prevede obligația de a efectua supraveghere video[7]. Cu toate acestea, dispozițiile cu cea mai mare probabilitate de a fi utilizate în practică sunt:

   - articolul 6 alineatul (1) litera (f) (interesul legitim);
   - articolul 6 alineatul (1) litera (e) (necesitatea de a îndeplini o sarcină care servește unui interes public sau care rezultă din exercitarea autorității publice).

În cazuri mai degrabă excepționale, operatorul ar putea utiliza ca temei juridic articolul 6 alineatul (1) litera (a) (consimțământul).

3.1 Interesul legitim, articolul 6 alineatul (1) litera (f)

17. Evaluarea juridică a articolului 6 alineatul (1) litera (f) ar trebui să se bazeze pe criteriile următoare, în conformitate cu considerentul 47.

3.1.1 Existența intereselor legitime

18. Supravegherea video este legală dacă este necesară pentru a îndeplini scopul unui interes legitim urmărit de un operator sau de o parte terță, cu excepția cazului în care interesele sau drepturile și libertățile fundamentale ale persoanei vizate prevalează asupra acestor interese [articolul 6 alineatul (1) litera (f)]. Interesele legitime urmărite de un operator sau de o parte terță pot fi interese juridice[8], economice sau morale[9]. Cu toate acestea, operatorul trebuie să ia în

[6] Normele referitoare la colectarea de probe pentru acțiunile civile variază de la un stat membru la altul.

[7] Prezentul ghid nu analizează și nu detaliază legislațiile naționale care ar putea fi diferite de la un stat membru la altul.

[8] Curtea de Justiție a Uniunii Europene, Hotărârea în cauza C-13/16, Rīgas satiksme, 4 mai 2017.

[9] Vezi WP 217, Grupul de Lucru instituit prin articolul 29.

considerare faptul că, dacă persoana vizată se opune supravegherii în conformitate cu articolul 21, operatorul poate continua supravegherea video a persoanei vizate respective doar dacă este un interes legitim *imperios* care prevalează asupra intereselor, drepturilor și libertăților persoanei vizate sau care vizează constatarea, exercitarea sau apărarea unui drept în instanță.

19. În cazul unei situații reale și periculoase, scopul protejării proprietății împotriva spargerii, furtului sau vandalismului poate constitui un interes legitim pentru supravegherea video.

20. Interesul legitim trebuie să existe cu adevărat și să fie o chestiune actuală (adică nu trebuie să fie fictiv sau speculativ)[10]. Înainte de începerea supravegherii trebuie să fi existat o situație reală de pericol - cum ar fi daune sau incidente grave produse în trecut. Având în vedere principiul răspunderii, ar fi indicat ca operatorii să documenteze incidentele relevante (data, modalitatea, pierderea financiară) și acuzațiile de natură penală aferente. Aceste incidente documentate pot fi o dovadă solidă a existenței unui interes legitim. Existența unui interes legitim, precum și necesitatea monitorizării trebuie reevaluate la intervale periodice (de exemplu, o dată pe an, în funcție de circumstanțe).

> Exemplu: Proprietarul unui magazin dorește să deschidă un nou magazin și vrea să instaleze un sistem de supraveghere video pentru a preveni vandalismul. Prin prezentarea de statistici, el poate demonstra că există o mare probabilitate de vandalism în vecinătate. De asemenea, este utilă experiența magazinelor din vecinătate. Nu este necesar ca operatorul în cauză să fi suferit un prejudiciu, de vreme ce prejudiciile înregistrate în vecinătate sugerează un pericol sau ceva asemănător și, prin urmare, pot indica un interes legitim. Cu toate acestea, nu este suficientă prezentarea statisticilor privind criminalitatea la nivel național sau general fără analizarea zonei în cauză sau a pericolelor la adresa magazinului respectiv.

21.

22. Situațiile care prezintă pericole iminente pot constitui un interes legitim, cum ar fi băncile sau magazinele care vând bunuri de valoare (de exemplu, bijuterii) sau zonele cunoscute ca fiind predilecte pentru infracțiuni contra patrimoniului (de exemplu, benzinăriile).

23. RGPD prevede în mod clar că autoritățile publice nu pot prelucra datele cu caracter personal în temeiul interesului legitim atâta timp cât se află în îndeplinirea atribuțiilor lor, potrivit articolului 6 alineatul (1) teza 2.

3.1.2 Necesitatea prelucrării

24. Datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”), vezi articolul 5 alineatul (1) litera (c). Înainte de instalarea unui sistem de supraveghere video, operatorul trebuie întotdeauna să examineze critic dacă această măsură este, în primul rând, adecvată pentru îndeplinirea obiectivului dorit și, în al doilea rând, adecvată și necesară pentru scopurile sale. Măsurile de supraveghere video trebuie selectate numai dacă scopul prelucrării nu ar putea fi îndeplinit în mod rezonabil prin alte mijloace, mai puțin invazive față de drepturile și libertățile fundamentale ale persoanei vizate.

25. În situația în care un operator dorește să prevină infracțiuni contra patrimoniului, în loc să instaleze un sistem de supraveghere video, acesta ar putea să ia măsuri alternative de securitate,

[10] Vezi WP 217, Grupul de Lucru instituit prin articolul 29, p. 24 și următoarele. Vezi și cauza CJUE C-708/18, p. 44.

cum ar fi împrejmuirea proprietății, instituirea de patrule regulate ale personalului de securitate, utilizarea de portari, asigurarea unei iluminări mai bune, montarea de încuietori de siguranță, ferestre și uși antiefracție sau aplicarea pe pereți a unei tencuieli sau folii antigraffiti. Aceste măsuri pot fi la fel de eficiente împotriva spargerii, furtului și vandalismului ca și sistemele de supraveghere video. Operatorul trebuie să evalueze de la caz la caz dacă astfel de măsuri pot fi o soluție rezonabilă.

26. Înainte de a folosi un sistem de camere, operatorul este obligat să stabilească unde și când sunt strict necesare măsurile de supraveghere video. De obicei, un sistem de supraveghere care funcționează pe timpul nopții, precum și în afara programului de lucru obișnuit, răspunde nevoilor operatorului pentru prevenirea oricărui pericol la adresa proprietății sale.

27. În general, necesitatea utilizării supravegherii video pentru protejarea spațiilor operatorului nu depășește limitele proprietății.[11] Cu toate acestea, există cazuri în care supravegherea proprietății nu este suficientă pentru o protecție eficientă. În unele cazuri individuale poate fi necesară extinderea supravegherii video la împrejurimile imediate ale proprietății. În acest context, operatorul trebuie să ia în considerare mijloace fizice și tehnice, de exemplu blocarea sau pixelarea zonelor nerelevante.

> Exemplu: O librărie dorește să-și protejeze sediul împotriva vandalismului. În general, camerele trebuie să filmeze doar spațiul respectiv deoarece nu este necesară supravegherea spațiilor învecinate sau a zonelor publice din împrejurimile sediului librăriei în acest scop.

28.

29. Întrebări referitoare la necesitatea prelucrării apar și în legătură cu modul în care sunt păstrate probele. În unele cazuri ar putea fi necesară folosirea unor soluții de tip „cutie neagră”, caz în care filmarea este ștearsă automat după o anumită perioadă de stocare și este accesată numai în cazul unui incident. În alte situații s-ar putea să nu fie necesară înregistrarea materialului video, fiind mai adecvată în schimb utilizarea monitorizării în timp real. Opțiunea între soluțiile de tip cutie neagră și monitorizarea în timp real ar trebui să corespundă și scopului urmărit. Dacă, de exemplu, scopul supravegherii video este păstrarea dovezilor, atunci metodele de monitorizare în timp real nu sunt adecvate. Uneori, monitorizarea în timp real poate fi și mai invazivă decât stocarea și ștergerea automată a materialului după un interval de timp limitat (de exemplu, dacă cineva urmărește permanent monitorul, monitorizarea poate fi mai invazivă decât atunci când nu există niciun monitor, iar materialul este stocat direct într-o cutie neagră). Principiul reducerii la minimum a datelor trebuie interpretat în acest context [articolul 5 alineatul (1) litera (c)]. De asemenea, trebuie avut în vedere că ar putea fi posibil ca, în locul supravegherii video, operatorul să utilizeze personal de securitate, care să poată reacționa și interveni imediat.

3.1.3 Asigurarea unui echilibru între interese

30. Presupunând că supravegherea video este necesară pentru a proteja interesele legitime ale unui operator, un sistem de supraveghere video poate fi pus în funcțiune numai dacă interesele sau drepturile și libertățile fundamentale ale persoanei vizate nu prevalează asupra intereselor legitime ale operatorului sau ale unei părți terțe (de exemplu, protejarea proprietății sau a integrității fizice). Operatorul trebuie să ia în considerare 1) în ce măsură monitorizarea afectează interesele, drepturile și libertățile fundamentale ale persoanelor și 2) dacă acest lucru provoacă încălcări ale drepturilor persoanei vizate sau consecințe negative cu privire la acestea. De fapt,

[11] Acest lucru ar putea, de asemenea, să facă obiectul legislației naționale în unele state membre.

evaluarea comparativă a intereselor este obligatorie. Drepturile și libertățile fundamentale, pe de o parte, și interesele legitime ale operatorului, pe de alta, trebuie evaluate și comparate cu atenție.

Exemplu: O firmă de parcare privată a documentat problemele recurente constând în furturi din mașinile parcate. Zona de parcare este un spațiu deschis și poate fi accesată cu ușurință de oricine, dar este semnalizată în mod clar cu indicatoare și blocante rutiere care delimitează spațiul. Firma de parcare are un interes legitim (prevenirea furturilor din mașinile clienților) de monitorizare a zonei în intervalul din zi în care se confruntă cu probleme. Persoanele vizate sunt monitorizate într-un interval de timp limitat, nu se află în zonă în scop recreativ și, de asemenea, este în interesul lor ca furturile să fie prevenite. În acest caz, interesul legitim al operatorului prevalează asupra interesului persoanelor vizate de a nu fi monitorizate.

Exemplu: Un restaurant decide să instaleze camere video în toalete pentru a controla curățenia instalațiilor sanitare. În acest caz, drepturile persoanelor vizate prevalează în mod clar asupra interesului operatorului, prin urmare nu pot fi instalate camere de luat vederi în astfel de locuri.

31.

3.1.3.1 Luarea deciziilor de la caz la caz

32. Întrucât evaluarea comparativă a intereselor este obligatorie în conformitate cu regulamentul, decizia trebuie luată de la caz la caz [vezi articolul 6 alineatul (1) litera (f)]. Trimiterea la situații abstracte sau compararea unor cazuri similare este insuficientă. Operatorul trebuie să evalueze riscurile de intruziune asupra drepturilor persoanei vizate; în acest caz, criteriul decisiv este intensitatea intervenției pentru drepturile și libertățile persoanei.

33. Intensitatea poate fi definită, printre altele, prin tipul de informații culese (conținutul informațiilor), sfera de aplicare (densitatea informației, dimensiunea spațială și geografică), numărul persoanelor vizate în cauză, fie ca număr specific, fie ca proporție din populația relevantă, situația în cauză, interesele reale ale grupului de persoane vizate, mijloacele alternative, precum și prin natura și domeniul evaluării datelor.

34. Factorii importanți de evaluare comparativă pot fi dimensiunea zonei aflate sub supraveghere și numărul persoanelor vizate supravegheate. Utilizarea supravegherii video într-o zonă izolată (de exemplu, pentru a urmări fauna sălbatică sau a proteja infrastructura critică, de exemplu o antenă radio privată) trebuie evaluată în mod diferit de supravegherea video dintr-o zonă pietonală sau dintr-un centru comercial.

1. Exemplu: Dacă se instalează o cameră auto (de exemplu, în scopul culegerii de dovezi în caz de accident), este important să se asigure faptul că această cameră nu înregistrează în permanență traficul și persoanele care se află în apropierea drumului. În caz contrar, interesul ca înregistrările video să constituie o dovadă în cazul mai teoretic al unui accident rutier nu poate justifica această interferență gravă cu drepturile persoanelor vizate[11].

35.

3.1.3.2 Așteptările rezonabile ale persoanelor vizate

36. Potrivit Considerentului 47, existența unui interes legitim necesită o evaluare atentă. Aici trebuie incluse așteptările rezonabile ale persoanei vizate din momentul și în contextul prelucrării datelor sale cu caracter personal. În ceea ce privește monitorizarea sistematică, relația dintre persoana vizată și operator poate varia semnificativ și poate afecta așteptările rezonabile pe care

le-ar putea avea persoana vizată. Interpretarea conceptului de așteptări rezonabile nu trebuie să se bazeze doar pe așteptările subiective în cauză. În schimb, criteriul decisiv trebuie să existe dacă o parte terță obiectivă ar putea să se aștepte în mod rezonabil și să decidă să facă obiectul monitorizării în această situație specifică.

37. De exemplu, în majoritatea cazurilor este puțin probabil ca un angajat să se aștepte să fie monitorizat de angajatorul său la locul de muncă[12]. De asemenea, nu este de așteptat să existe monitorizare în grădina privată a unei persoane, în spații de locuit sau în săli de examinare și de tratament. În aceeași ordine de idei, nu este rezonabil să se preconizeze existența monitorizării la grupurile sanitare sau la saună - monitorizarea unor astfel de zone este o intruziune intensă asupra drepturilor persoanei vizate. Persoanele vizate se așteaptă în mod rezonabil ca în zonele respective să nu existe supraveghere video. Pe de altă parte, clientul unei bănci s-ar putea aștepta să fie monitorizat în incinta băncii sau la bancomat.

38. De asemenea, persoanele vizate se pot aștepta să nu fie monitorizate în zonele accesibile publicului, mai ales dacă aceste zone sunt folosite în mod obișnuit pentru activități de recuperare, regenerare și recreere, precum și în locurile în care persoanele stau și/sau comunică, de exemplu în zone de odihnă, la mese de restaurant, în parcuri, la cinematografe și în centre de fitness. În aceste situații, interesele sau drepturile și libertățile persoanei vizate vor prevala deseori asupra intereselor legitime ale operatorului.

> Exemplu: Persoanele vizate se așteaptă să nu fie monitorizate la toaletă. Supravegherea video pentru prevenirea accidentelor, de exemplu, nu este proporțională.

39.

40. Semnele care informează persoana vizată cu privire la supravegherea video nu au nicio relevanță atunci când se stabilește la ce se poate aștepta în mod obiectiv o persoană vizată. Aceasta înseamnă că, de exemplu, proprietarul unui magazin nu poate miza pe așteptarea rezonabilă pe care clienții ar avea-o *în mod obiectiv* de a fi monitorizați doar pentru că există un semn la intrare care îi informează cu privire la supraveghere.

3.2 Necesitatea aducerii la îndeplinire a unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, articolul 6 alineatul (1) litera (e).

41. Datele cu caracter personal ar putea fi prelucrate prin supraveghere video în temeiul articolului 6 alineatul (1) litera (e) dacă prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice[13]. S-ar putea ca exercitarea autorității publice să nu permită o astfel de prelucrare, dar alte temeiuri legislative, cum ar fi „sănătatea și siguranța” pentru protecția vizitatorilor și a angajaților, pot oferi un domeniu limitat pentru prelucrare, având în vedere în același timp obligațiile care decurg din RGPD și drepturile persoanei vizate.

[12] Vezi și: Grupul de Lucru instituit prin articolul 29, Avizul 2/2017 privind prelucrarea datelor la locul de muncă, WP 249, adoptat la 8 iunie 2017.

[13] Temeiul prelucrării menționate este prevăzut de dreptul Uniunii sau de dreptul statului membru și este necesar pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul [articolul 6 alineatul (3)].

42. Statele membre pot menține sau introduce legislații naționale specifice privind supravegherea video pentru a adapta aplicarea normelor RGPD prin stabilirea unor cerințe specifice mai exacte pentru prelucrare, atâta timp cât aceasta este în conformitate cu principiile prevăzute de RGPD (de exemplu, limitările legate de stocare, proporționalitatea).

3.3 Consimțământul, articolul 6 alineatul (1) litera (a)

43. Consimțământul trebuie să fie acordat în mod liber, specific, în cunoștință de cauză și lipsit de ambiguitate, astfel cum este descris în Ghidul privind consimțământul[14].

44. În ceea ce privește monitorizarea sistematică, consimțământul persoanei vizate nu poate servi ca temei juridic în conformitate cu articolul 7 (vezi considerentul 43) decât în cazuri excepționale. Prin natura supravegherii, această tehnologie monitorizează simultan un număr necunoscut de persoane. Va fi dificil pentru operator să poată să demonstreze că persoana vizată și-a dat consimțământul înainte de prelucrarea datelor sale personale [articolul 7 alineatul (1)]. Presupunând că persoana vizată își retrage consimțământul, va fi dificil pentru operator să demonstreze că datele cu caracter personal nu mai sunt prelucrate [articolul 7 alineatul (3)].

> Exemplu: Sportivii pot solicita monitorizarea în timpul exercițiilor individuale pentru a-și analiza tehnicile și performanțele. Pe de altă parte, atunci când un club sportiv ia inițiativa de a monitoriza o întreagă echipă în același scop, deseori consimțământul nu va fi valabil, deoarece sportivii se pot simți presați să-și dea consimțământul la nivel individual, pentru ca refuzul lor să nu-i afecteze negativ pe coechipieri.

45.

46. Dacă operatorul dorește să aibă consimțământul, este de datoria sa să se asigure că orice persoană vizată care intră în zona aflată sub supraveghere video și-a dat consimțământul. Consimțământul trebuie să îndeplinească condițiile prevăzute la articolul 7. Intrarea într-o zonă monitorizată marcată (de exemplu, oamenii sunt invitați să treacă printr-un anumit coridor sau o poartă pentru a intra într-o zonă monitorizată) nu constituie o declarație sau o acțiune afirmativă clară necesară pentru consimțământ, cu excepția cazului în care sunt îndeplinite criteriile prevăzute la articolele 4 și 7, astfel cum sunt descrise în Ghidul privind consimțământul[15].

47. Având în vedere dezechilibrul de putere dintre angajatori și angajați, în majoritatea cazurilor, angajatorii nu trebuie să se bazeze pe consimțământ atunci când prelucrează date cu caracter personal, deoarece este puțin probabil ca acesta să fie acordat în mod liber. În acest context trebuie avut în vedere Ghidul privind consimțământul.

48. Legea sau acordurile colective ale statelor membre, inclusiv „acordurile de muncă”, pot prevedea norme detaliate cu privire la prelucrarea datelor cu caracter personal ale angajaților în contextul ocupării unui loc de muncă (vezi articolul 88).

[14] Grupul de lucru instituit prin articolul 29, Ghid privind consimțământul conform Regulamentului 2016/679 (WP 259 rev. 01) - aprobat de CEPD.

[15] Grupul de lucru instituit prin articolul 29, Ghid privind consimțământul conform Regulamentului 2016/679 (WP 259) - aprobat de CEPD - care trebuie avut în vedere.

4 DIVULGAREA ÎNREGISTRĂRILOR VIDEO CĂTRE PĂRȚI TERȚE

49. În principiu, în cazul divulgării înregistrărilor video către părți terțe se aplică reglementările generale ale RGPD.

4.1 Divulgarea înregistrărilor video către părți terțe în general

50. Divulgarea este definită la articolul 4 alineatul (2) ca transmitere (de exemplu, comunicare individuală), diseminare (de exemplu, publicare online) sau punere la dispoziție în orice alt mod. Părțile terțe sunt definite la articolul 4 alineatul (10). În cazul în care divulgarea se face către țări terțe sau organizații internaționale, se aplică și dispozițiile speciale de la articolul 44 și următoarele.

51. Orice divulgare a datelor cu caracter personal este un mod separat de prelucrare a datelor cu caracter personal pentru care operatorul trebuie să aibă un temei juridic prevăzut la articolul 6.

> Exemplu: Un operator care dorește să încarce o înregistrare pe internet trebuie să se bazeze pe un temei juridic pentru prelucrarea respectivă, de exemplu, obținând consimțământul persoanei vizate în conformitate cu articolul 6 alineatul (1) litera (a).

52.

53. Transmiterea înregistrărilor video către părți terțe în alt scop decât cel pentru care au fost culese datele este posibilă în conformitate cu normele prevăzute la articolul 6 alineatul (4).

> Exemplu: Supravegherea video a unei bariere (la o parcare) este instalată în scopul soluționării daunelor. Se produce o daună, iar înregistrarea este transmisă unui avocat pentru a deschide un dosar. În acest caz, scopul înregistrării este același cu cel al transmiterii.
>
> Exemplu: Supravegherea video a unei bariere (la o parcare) este instalată în scopul soluționării daunelor. Înregistrarea este publicată online, exclusiv pentru amuzament. În acest caz, scopul s-a schimbat și nu este compatibil cu scopul inițial. În plus, ar fi problematic să se identifice un temei juridic pentru această prelucrare (publicarea).

54.

55. O parte terță destinatară va trebui să realizeze propria analiză juridică, în special să-și identifice temeiul juridic în conformitate cu articolul 6 pentru prelucrarea pe care o realizează (de exemplu, primirea materialului).

4.2 Divulgarea înregistrărilor video către autoritățile de aplicare a legii

56. Divulgarea înregistrărilor video către autoritățile de aplicare a legii este, de asemenea, un proces independent, care necesită o justificare separată pentru operator.

57. Conform articolului 6 alineatul (1) litera (c), prelucrarea este legală dacă este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului. Deși legislația aplicabilă poliției se află sub controlul exclusiv al statelor membre, cel mai probabil există norme generale care reglementează transferul probelor către autoritățile de aplicare a legii în fiecare stat membru. Prelucrarea constând în transmiterea datelor de către operator este reglementată de RGPD. Dacă legislația națională impune operatorului să coopereze cu autoritățile de aplicare a legii (de exemplu, în cadrul unei anchete), temeiul juridic pentru transmiterea datelor este obligația legală prevăzută la articolul 6 alineatul (1) litera (c).

58. Limitarea scopului prevăzută la articolul 6 alineatul (4) este adesea neproblematică, întrucât divulgarea se referă în mod explicit la dreptul intern. Prin urmare, nu este necesară o examinare a cerințelor speciale pentru o schimbare de scop în sensul literelor (a)-(e).

> Exemplu: Proprietarul unui magazin înregistrează imagini la intrare. În imagini se vede o persoană care fură portofelul alteia. Poliția solicită operatorului să predea materialul pentru a fi folosit în anchetă. În acest caz, proprietarul magazinului ar utiliza temeiul juridic prevăzut la articolul 6 alineatul (1) litera (c) (obligația legală) interpretat în coroborare cu dreptul intern relevant pentru prelucrarea prin transfer.

59.

> Exemplu: Într-un magazin se instalează o cameră de luat vederi din motive de securitate. Proprietarul magazinului consideră că a surprins ceva suspect în materialele înregistrate și decide să le trimită poliției (fără niciun indiciu că ar exista o anchetă în curs, de orice natură). În acest caz, proprietarul magazinului trebuie să evalueze dacă sunt îndeplinite condițiile prevăzute, în majoritatea cazurilor, la articolul 6 alineatul (1) litera (f). De obicei, acest lucru este valabil dacă proprietarul magazinului are o suspiciune rezonabilă legată de comiterea unei infracțiuni.

60.

61. Prelucrarea datelor cu caracter personal de către autoritățile de aplicare a legii nu respectă RGPD [vezi articolul 2 alineatul (2) litera (d)], ci este, în schimb, conformă cu Directiva privind protecția datelor în contextul aplicării legii [(UE) 2016/680].

5 PRELUCRAREA DE CATEGORII SPECIALE DE DATE

62. Sistemele de supraveghere video colectează de obicei cantități masive de date cu caracter personal, care pot dezvălui informații extrem de personale și chiar categorii speciale de date. Într-adevăr, date aparent nesemnificative colectate inițial prin mijloace video pot fi folosite pentru a deduce alte informații în vederea atingerii unui scop diferit (de exemplu, pentru a urmări obiceiurile unei persoane). Cu toate acestea, supravegherea video nu este întotdeauna considerată prelucrare de categorii speciale de date cu caracter personal.

> Exemplu: Înregistrările video în care se vede o persoană vizată purtând ochelari sau utilizând un fotoliu rulant nu sunt considerate în sine categorii speciale de date cu caracter personal.

63.

64. Cu toate acestea, dacă materialul video este prelucrat pentru a deduce categorii speciale de date, se aplică articolul 9.

> Exemplu: Opiniile politice ar putea fi deduse, de exemplu, din imagini care prezintă persoane vizate identificabile participând la un eveniment, luând parte la o grevă, etc. Această situație ar intra sub incidența articolului 9.
>
> Exemplu: Instalarea unei camere video de către un spital pentru a monitoriza starea de sănătate a unui pacient ar fi considerată prelucrare de categorii speciale de date cu caracter personal (articolul 9).

65.

66. În general, ca principiu, de fiecare dată când se instalează un sistem de supraveghere video trebuie să ia în considerare principiul reducerii la minimum a datelor. Prin urmare, chiar și în cazurile în care nu se aplică articolul 9 alineatul (1), operatorul de date trebuie să încerce întotdeauna să reducă la minimum riscul de a capta imagini care dezvăluie alte date cu caracter special (dincolo de sfera articolului 9), indiferent de scop.

> Exemplu: Supravegherea video care surprinde o biserică nu intră în sine sub incidența articolului 9. Cu toate acestea, operatorul trebuie să efectueze o evaluare deosebit de atentă în baza articolului 6 alineatul (1) litera (f), ținând seama de natura datelor, precum și de riscul de înregistrare a altor date cu caracter special (dincolo de sfera articolului 9) atunci când sunt evaluate interesele persoanei vizate.

67.

68. Dacă un sistem de supraveghere video este utilizat pentru a prelucra categorii speciale de date, operatorul de date trebuie să identifice atât o excepție pentru prelucrarea categoriilor speciale de date în baza articolului 9 (adică o excepție de la regula generală conform căreia nu trebuie prelucrate categoriile speciale de date), cât și un temei juridic în conformitate cu articolul 6.

69. De exemplu, articolul 9 alineatul (2) litera (c) („[…] *prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice* […]") ar putea – în mod teoretic și excepțional – să fie utilizat, dar operatorul de date ar trebui să justifice prelucrarea prin necesitatea absolută de a proteja interesele vitale ale unei persoane și să demonstreze că această „[…] persoană vizată *se află în incapacitate fizică sau juridică de a-și da consimțământul*". În plus, operatorul de date nu va avea permisiunea să folosească sistemul pentru orice alt motiv.

70. Este important de menționat aici că este improbabil ca orice excepție enumerată la articolul 9 să fie utilizabilă pentru a justifica prelucrarea categoriilor speciale de date prin supraveghere video. Mai precis, operatorii de date care prelucrează aceste date în contextul supravegherii video nu se pot baza pe articolul 9 alineatul (2) litera (e), care permite prelucrarea datelor cu caracter personal care sunt făcute publice în mod evident de către persoana vizată. Simplul fapt de a intra în raza camerei de luat vederi nu implică faptul că persoana vizată intenționează să facă publice categoriile speciale de date referitoare la sine.

71. De asemenea, pentru prelucrarea categoriilor speciale de date este necesară o vigilență sporită și permanentă față de anumite obligații; de exemplu, un nivel ridicat de securitate și o evaluare a impactului asupra protecției datelor, dacă este necesar.

> Exemplu: Un angajator nu poate să folosească înregistrări ale supravegherii video care prezintă o demonstrație cu scopul de a identifica greviștii.

72.

5.1 Considerații generale la prelucrarea datelor biometrice

73. Utilizarea datelor biometrice și, în special, recunoașterea facială implică riscuri crescute pentru drepturile persoanelor vizate. Este esențial ca astfel de tehnologii să fie utilizate respectându-se principiul legalității, al necesității, al proporționalității și al reducerii la minimum a datelor, prevăzute în RGPD. Chiar dacă utilizarea acestor tehnologii poate fi percepută ca deosebit de eficientă, operatorii trebuie să evalueze în primul rând impactul asupra drepturilor și libertăților fundamentale și să ia în considerare mijloace mai puțin invazive pentru a-și atinge scopul legitim al prelucrării.

74. Pentru a se încadra în datele biometrice definite în RGPD, prelucrarea datelor brute, cum ar fi caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, trebuie să implice măsurarea acestor caracteristici. Întrucât datele biometrice sunt rezultatul unor astfel de măsurători, RGPD afirmă la articolul 4 alineatul (14) că acestea *„[…] rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice, care permit sau confirmă identificarea unică a respectivei persoane […]”.* Înregistrările video ale unei persoane nu pot fi, însă, considerate în sine date biometrice în conformitate cu articolul 9 dacă nu au fost prelucrate prin tehnici specifice pentru a contribui la identificarea unei persoane[16].

75. Pentru a putea fi considerată prelucrare de categorii speciale de date cu caracter personal (articolul 9), datele biometrice trebuie să fie prelucrate „pentru identificarea unică a unei persoane fizice”.

76. În consecință, având în vedere articolul 4 alineatul (14) și articolul 9, trebuie luate în considerare trei criterii:

- **Natura datelor:** date referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice,

[16] Considerentul 51 din RGPD sprijină această analiză, afirmând că *„[…] Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice […]*”.

- **Mijloacele și modul de prelucrare**: date care „rezultă în urma unor tehnici de prelucrare specifice”,

- **Scopul prelucrării:** datele trebuie să fie utilizate pentru identificarea unică a unei persoane fizice.

77. Utilizarea supravegherii video, inclusiv funcționalitatea de recunoaștere biometrică instalată de către entități private în scopuri proprii (de exemplu, marketing, statistică sau chiar securitate) va necesita, în cele mai multe cazuri, consimțământul explicit din partea tuturor persoanelor vizate [articolul 9 alineatul (2) litera (a)]; cu toate acestea, se poate aplica și o altă excepție adecvată prevăzută la articolul 9.

2. Exemplu: Pentru a-și îmbunătăți serviciile, o companie privată înlocuiește punctele de verificare a identității pasagerilor dintr-un aeroport (preluarea bagajelor, îmbarcarea) cu sisteme de supraveghere video care utilizează tehnici de recunoaștere facială pentru a verifica identitatea pasagerilor care au ales să consimtă la o astfel de procedură. Întrucât prelucrarea intră sub incidența articolului 9, pasagerii, care și-au dat anterior consimțământul explicit și în cunoștință de cauză, vor trebui să se înscrie, de exemplu, la un terminal automat pentru a-și crea și înregistra modelul facial asociat cu cartea de îmbarcare și identitatea lor. Punctele de control curecunoaștere facială trebuie să fie clar delimitate, de exemplu, sistemul trebuie instalat într-un spațiu separat, pentru a nu fi captate modelele biometrice ale unei persoane care nu consimte la acest lucru. Doar pasagerii care și-au dat în prealabil consimțământul și au continuat procesul de înregistrare vor folosi spațiul echipat cu sistemul biometric.

3. Exemplu: Un operator gestionează accesul la clădirea sa folosind o metodă de recunoaștere facială. Oamenii pot utiliza acest mod de acces numai dacă și-au dat în prealabil consimțământul explicit și în cunoștință de cauză [în conformitate cu articolul 9 alineatul (2) litera (a)]. Cu toate acestea, pentru a se asigura că nu se captează imaginea niciunei persoane care nu și-a dat anterior consimțământul, metoda recunoașterii faciale ar trebui utilizată chiar de către persoana vizată, de exemplu prin apăsarea unui buton. Pentru a asigura legalitatea prelucrării datelor, operatorul trebuie să ofere întotdeauna o modalitate alternativă de acces în clădire, fără prelucrare biometrică, cum ar fi legitimații sau chei.

78.

79. În acest tip de cazuri, în care sunt generate modele biometrice, operatorii se asigură că, după obținerea unui rezultat (potrivire sau nepotrivire), toate modelele intermediare realizate (cu acordul explicit și în cunoștință de cauză al persoanei vizate) pentru a fi comparate cu cele create de persoanele vizate la momentul înregistrării sunt șterse imediat și în condiții de siguranță. Modelele create pentru înregistrare trebuie păstrate numai pentru realizarea scopului prelucrării și nu trebuie stocate sau arhivate.

80. Totuși, atunci când scopul prelucrării este, de exemplu, distingerea unei categorii de persoane de alta, fără a identifica în mod unic pe nimeni, prelucrarea nu intră sub incidența articolului 9.

4. Exemplu: Proprietarul unui magazin dorește să-și personalizeze oferta pe baza caracteristicilor de gen și vârstă ale clientelei înregistrare de un sistem de supraveghere video. Dacă acest sistem nu generează modele biometrice pentru a identifica în mod unic persoanele, ci doar detectează caracteristicile fizice necesare pentru a clasifica persoanele, atunci prelucrarea nu intră sub incidența articolului 9 (atâta timp cât nu sunt prelucrate alte tipuri de categorii speciale de date).

81.

82. Totuși, articolul 9 se aplică dacă operatorul stochează date biometrice [cel mai frecvent prin modele create prin extragerea caracteristicilor cheie din forma brută a datelor biometrice (de exemplu, măsurători faciale dintr-o imagine)] pentru a identifica în mod unic o persoană. Dacă un operator dorește să detecteze o persoană vizată care reintră în zonă sau intră în altă zonă (de exemplu, pentru a proiecta reclame personalizate suplimentare), scopul ar fi în acest caz identificarea unică a unei persoane fizice, ceea ce înseamnă că operațiunea ar intra de la început sub incidența articolului 9. Acesta ar putea fi cazul unui operator care stochează modelele generate pentru a afișa reclame adaptate suplimentare pe mai multe panouri publicitare în diferite locuri din magazin. Întrucât sistemul folosește caracteristici fizice pentru a detecta anumite persoane care revin în raza camerei de luat vederi (cum ar fi vizitatorii unui centru comercial) și le urmărește, aceasta ar constitui o metodă de identificare biometrică, deoarece are ca scop recunoașterea prin utilizarea unor tehnici de prelucrare specifice.

5. Exemplu: Proprietarul unui magazin a instalat un sistem de recunoaștere facială în interiorul magazinului său pentru a-și personaliza oferta adresată persoanelor fizice. Operatorul de date trebuie să obțină consimțământul explicit și în cunoștință de cauză al tuturor persoanelor vizate înainte de a utiliza acest sistem biometric și de a difuza reclame personalizate. Sistemul ar fi ilegal dacă ar capta imagini cu vizitatori sau trecători care nu au consimțit la crearea modelului lor biometric, chiar dacă modelul respectiv este șters în cel mai scurt timp. Într-adevăr, aceste modele temporare constituie date biometrice prelucrate pentru a identifica în mod unic o persoană care poate nu dorește să facă obiectul reclamelor personalizate.

83.

84. CEPD observă că unele sisteme biometrice sunt instalate în medii necontrolate[17], ceea ce înseamnă că sistemul captează imagini cu fața oricărei persoane care trece prin raza camerei, inclusiv a persoanelor care nu au consimțit la dispozitivul biometric, creând astfel modele biometrice. Aceste modele sunt comparate cu cele create pentru persoanele vizate care și-au dat consimțământul în prealabil în cursul unui proces de înregistrare (adică utilizatorii dispozitivului biometric), pentru ca operatorul de date să recunoască dacă persoana este sau nu un utilizator al dispozitivului biometric. În acest caz, sistemul este deseori conceput astfel încât să facă distincția între persoanele pe care dorește să le recunoască dintr-o bază de date și cele care nu sunt înregistrate. Întrucât scopul este identificarea unică a persoanelor fizice, este necesară, totuși, o excepție în temeiul articolului 9 alineatul (2) din RGPD pentru orice persoană înregistrată de cameră.

[17] Aceasta înseamnă că dispozitivul biometric este amplasat într-un spațiu deschis publicului și poate să acționeze asupra tuturor trecătorilor, spre deosebire de sistemele biometrice din medii controlate, care pot fi utilizate numai prin participarea persoanei care consimte la acest lucru.

6. Exemplu: Un hotel folosește supraveghere video pentru a avertiza automat administratorul hotelului că a sosit o persoană foarte importante (VIP) atunci când este recunoscută fața clientului. Aceste VIP-uri au prioritate, dat fiind că și-au dat consimțământul explicit pentru utilizarea recunoașterii faciale înainte de a fi înregistrate într-o bază de date instituită în acest scop. Astfel de sisteme de prelucrare a datelor biometrice ar fi ilegale, cu excepția cazului în care toți ceilalți clienți monitorizați (pentru identificarea VIP-urilor) au consimțit la prelucrare în conformitate cu articolul 9 alineatul (2) litera (a) din RGPD.

7. Exemplu: Un operator instalează un sistem de supraveghere video cu recunoaștere facială la intrarea în sala de concerte pe care o administrează. Operatorul trebuie să organizeze intrări clar delimitate, una cu un sistem biometric și alta fără acest sistem (unde, de exemplu, se scanează un bilet). Intrările dotate cu dispozitive biometrice trebuie instalate și puse la dispoziție într-un mod care să împiedice sistemul să înregistreze modelele biometrice ale spectatorilor care nu consimt la acest lucru.

85.

86. În fine, atunci când consimțământul este impus de articolul 9 din RGPD, operatorul de date nu trebuie să condiționeze accesul la serviciile sale în funcție de acceptarea prelucrării biometrice. Cu alte cuvinte și în special atunci când prelucrarea biometrică este utilizată în scop de autentificare, operatorul de date trebuie să ofere o soluție alternativă care să nu implice prelucrarea biometrică - fără restricții sau costuri suplimentare pentru persoana vizată. Această soluție alternativă este necesară și pentru persoanele care nu îndeplinesc constrângerile dispozitivului biometric (înregistrare sau citire a datelor biometrice imposibilă, situație de dizabilitate care face dificilă utilizarea etc.) și pentru situația indisponibilității dispozitivului biometric (cum ar fi o defecțiune a dispozitivului); trebuie aplicată o „soluție de rezervă” pentru a asigura continuitatea serviciului propus, limitată însă la o utilizare excepțională. În cazuri excepționale, ar putea exista o situație în care prelucrarea datelor biometrice este activitatea principală a unui serviciu furnizat pe bază de contract, de exemplu, un muzeu care organizează o expoziție pentru a demonstra utilizarea unui dispozitiv de recunoaștere facială, caz în care persoana vizată nu va putea respinge prelucrarea datelor biometrice dacă dorește să participe la expoziție. În acest caz, consimțământul necesar în temeiul articolului 9 este, totuși, valabil dacă sunt îndeplinite cerințele prevăzute la articolul 7.

5.2 Măsuri propuse pentru reducerea la minimum a riscurilor cu privire la prelucrarea datelor biometrice

87. În conformitate cu principiul reducerii la minimum a datelor, operatorii de date trebuie să se asigure că datele extrase dintr-o imagine digitală pentru a construi un model nu vor fi excesive și vor conține numai informațiile necesare în scopul specificat, evitând astfel orice prelucrare suplimentară posibilă. Ar trebui instituite măsuri pentru a garanta că modelele nu pot fi transferate de la un sistem biometric la altul.

88. Identificarea și autentificarea/verificarea vor necesita, probabil, stocarea modelului pentru a fi utilizat ulterior în scopuri comparative. Operatorul de date trebuie să ia în considerare locul cel mai potrivit pentru stocarea datelor. Într-un mediu controlat (coridoare delimitate sau puncte de control), modelele trebuie stocate pe un dispozitiv individual aflat în posesia utilizatorului și sub controlul său exclusiv (printr-un telefon inteligent sau cu cartea de identitate) sau - atunci când este necesar în scopuri specifice și în cazul unor nevoi obiective - stocate într-o bază de date centralizată într-o formă criptată, accesibilă cu o cheie/metodă secretă folosită doar de persoana respectivă pentru a preveni accesul neautorizat la model sau la locul de stocare. În situația în

care nu poate evita accesul la modele, operatorul de date trebuie să ia măsurile adecvate pentru a asigura securitatea datelor stocate. O astfel de măsură poate fi criptarea modelului folosind un algoritm criptografic.

89. În orice caz, operatorul trebuie să ia toate precauțiile necesare pentru a păstra disponibilitatea, integritatea și confidențialitatea datelor prelucrate. În acest scop, operatorul va lua în special următoarele măsuri: compartimentarea datelor în timpul transmiterii și stocării, stocarea modelelor biometrice și a datelor brute sau a datelor de identitate în baze de date distincte, criptarea datelor biometrice, în special a modelelor biometrice, și definirea unei politici de criptare și gestionarea cheilor, integrarea unei măsuri organizatorice și tehnice pentru depistarea fraudei, asocierea unui cod de integritate cu datele (de exemplu, semnătură sau hash) și interzicerea accesului extern la datele biometrice. Astfel de măsuri trebuie să evolueze odată cu progresul tehnologiilor.

90. În plus, operatorii de date trebuie să ia măsuri pentru ștergerea datelor brute (imagini faciale, semnale vocale, mers etc.) și să asigure eficacitatea ștergerii. Dacă nu mai există un temei juridic pentru prelucrare, datele brute trebuie șterse. Într-adevăr, în măsura în care modelele biometrice derivă din astfel de date, crearea bazelor de date ar putea fi considerată drept o amenințare egală, dacă nu chiar mai mare (pentru că este posibil ca un model biometric să nu fie întotdeauna ușor de citit fără cunoașterea modului în care a fost programat, iar datele brute sunt elementele componente ale oricărui model). În cazul în care operatorul ar fi nevoit să păstreze aceste date, trebuie explorate metode care adaugă o componentă de tip zgomot aditiv (cum ar fi watermarkingul), ceea ce ar face ineficientă crearea modelului. De asemenea, operatorul trebuie să șteargă datele și modelele biometrice în caz de acces neautorizat la terminalul de citire-comparație sau la serverul de stocare și să șteargă datele care nu sunt utile pentru prelucrarea ulterioară la sfârșitul ciclului de viață a dispozitivului biometric.

6 DREPTURILE PERSOANEI VIZATE

91. Având în vedere caracterul prelucrării datelor atunci când se utilizează supravegherea video, pentru unele drepturi ale persoanei vizate conform RGPD sunt necesare clarificări suplimentare. Acest capitol nu este însă exhaustiv, toate drepturile prevăzute în RGPD se aplică prelucrării datelor cu caracter personal prin supraveghere video.

6.1 Dreptul de acces

92. O persoană vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal. În cazul supravegherii video, acest lucru înseamnă că, dacă datele nu sunt stocate sau transferate în niciun fel, după ce a trecut momentul monitorizării în timp real, operatorul nu poate să furnizeze decât informația că nu mai sunt prelucrate date cu caracter personal (pe lângă obligațiile de informare generală prevăzute la articolul 13, vezi *secțiunea 7 – Obligații privind transparența și informarea*). Dacă însă la momentul solicitării încă se prelucrează date (adică dacă datele sunt stocate sau prelucrate în continuare în orice alt mod), persoana vizată trebuie să primească acces și să fie informată în conformitate cu articolul 15.

93. Există, totuși, o serie de limitări care se pot aplica în unele cazuri în legătură cu dreptul de acces.

- Articolul 15 alineatul (4) din RGPD aduce atingere drepturilor altora.

94. Având în vedere că aceeași secvență din supravegherea video poate înregistra orice număr de persoane vizate, atunci o vizualizare ar duce la prelucrarea suplimentară a datelor cu caracter personal ale altor persoane vizate. Dacă persoana vizată dorește să primească o copie a materialului [articolul 15 alineatul (3)], acest lucru ar putea aduce atingere drepturilor și libertăților altor persoane vizate din material. Prin urmare, pentru a preveni acest efect, operatorul trebuie să ia în considerare faptul că, din cauza naturii invazive a înregistrărilor video, acestea nu trebuie furnizate, în unele cazuri, atunci când pot fi identificate alte persoane vizate. Protejarea drepturilor părților terțe nu trebuie însă folosită drept scuză pentru a împiedica solicitările legitime de acces ale persoanelor; în aceste cazuri, operatorul trebuie să pună în aplicare măsuri tehnice pentru a îndeplini cererea de acces (de exemplu, editarea imaginilor, cum ar fi mascarea sau distorsionarea). Operatorii nu sunt însă obligați să pună în aplicare astfel de măsuri tehnice dacă se pot asigura în alt mod că sunt capabili să răspundă unei solicitări efectuate în temeiul articolului 15 în termenul prevăzut la articolul 12 alineatul (3).

- Articolul 11 alineatul (2) din RGPD: operatorul nu este în măsură să identifice persoana vizată.

95. În cazul în care nu pot fi căutate date cu caracter personal în înregistrările video (adică operatorul ar trebui să parcurgă, probabil, un volum mare de materiale stocate pentru a găsi persoana vizată respectivă), operatorul poate să nu fie în măsură să identifice persoana vizată.

96. Din aceste motive, persoana vizată (pe lângă faptul că trebuie să se identifice, inclusiv cu documentul de identitate sau în persoană) trebuie să specifice în cererea sa către operator când anume - într-un interval de timp rezonabil proporțional cu numărul de persoane vizate înregistrate - a intrat în zona monitorizată. Operatorul trebuie să aducă, în prealabil, la cunoștința persoanei vizate informațiile necesare pentru îndeplinirea cererii. Dacă operatorul poate demonstra că nu este în măsură să identifice persoana vizată, trebuie să informeze persoana respectivă în consecință, dacă este posibil.

În această situație, în răspunsul său către persoana vizată, operatorul trebuie să furnizeze informații cu privire la zona exactă a monitorizării, verificarea camerelor care erau în funcțiune etc., pentru ca persoana vizată să înțeleagă pe deplin ce date personale este posibil să fi fost prelucrate.

> Exemplu: Dacă o persoană vizată solicită o copie a datelor sale personale prelucrate prin supraveghere video la intrarea într-un centru comercial cu 30 000 de vizitatori pe zi, persoana vizată trebuie să specifice când a trecut prin zona monitorizată într-un interval de aproximativ o oră. Dacă operatorul prelucrează încă materialul, trebuie să i se pună la dispoziție o copie a înregistrării video. Dacă alte persoane vizate pot fi identificate în același material, atunci acea parte a materialului trebuie anonimizată (de exemplu, prin estomparea copiei sau a unor părți ale acesteia) înainte de transmiterea copiei către persoana vizată care a depus cererea.
>
> Exemplu: Dacă operatorul șterge automat toate înregistrările video, de exemplu în termen de 2 zile, nu este în măsură să furnizeze înregistrarea persoanei vizate după cele 2 zile. Dacă operatorul primește o solicitare după cele 2 zile, persoana vizată trebuie informată în consecință.

97.

- Articolul 12 din RGPD: cereri excesive

98. În cazul unor cereri excesive sau vădit nefondate din partea unei persoane vizate, operatorul poate fie să perceapă o taxă rezonabilă în conformitate cu articolul 12 alineatul (5) litera (a) din RGPD, fie să refuze să dea curs cererii [articolul 12 alineatul (5) litera (b) din RGPD]. Operatorul trebuie să poată demonstra caracterul vădit nefondat sau excesiv al cererii.

6.2 Dreptul la ștergerea datelor și dreptul la opoziție

6.2.1 Dreptul la ștergerea datelor („dreptul de a fi uitat”)

99. Dacă operatorul continuă să prelucreze datele cu caracter personal ulterior monitorizării în timp real (de exemplu, prin stocare), persoana vizată poate solicita ștergerea datelor cu caracter personal în temeiul articolului 17 din RGPD.

100. La cerere, operatorul este obligat să șteargă datele cu caracter personal fără întârzieri nejustificate dacă se aplică una dintre circumstanțele enumerate la articolul 17 alineatul (1) din RGPD [și dacă nu se aplică niciuna din excepțiile enumerate la articolul 17 alineatul (3) din RGPD]. În acest caz este inclusă obligația de a șterge datele cu caracter personal când nu mai sunt necesare pentru îndeplinirea scopului pentru care au fost stocate inițial sau când prelucrarea este ilegală (vezi și *secțiunea 8 – Perioadele de stocare și obligația de ștergere a datelor*). În plus, în funcție de temeiul juridic al prelucrării, datele cu caracter personal trebuie șterse:

- *din motive legate de consimțământ*: ori de câte ori consimțământul este retras (și nu există alt temei juridic pentru prelucrare);
- *din motive legate de interesul legitim*:
  - ori de câte ori persoana vizată își exercită dreptul de a se opune (vezi *secțiunea 6.2.2*) și nu există motive legitime imperioase pentru prelucrare care să prevaleze sau
  - în caz de marketing direct (inclusiv crearea de profiluri), ori de câte ori persoana vizată se opune prelucrării.

101. Dacă operatorul a făcut publică înregistrarea video (de exemplu, prin televiziune sau streaming online), trebuie luate măsuri rezonabile pentru informarea celorlalți operatori (care prelucrează acum datele cu caracter personal în cauză) cu privire la cererea efectuată în conformitate cu articolul 17 alineatul (2) din RGPD. Măsurile rezonabile trebuie să includă măsuri tehnice, luând în considerare tehnologia disponibilă și costurile de implementare. În măsura în care este posibil, operatorul trebuie să notifice - în momentul ștergerii datelor cu caracter personal - orice persoană căreia i-au fost divulgate anterior datele cu caracter personal, în conformitate cu articolul 19 din RGPD.

102. Pe lângă obligația de a șterge datele cu caracter personal la solicitarea persoanei vizate, operatorul este obligat să limiteze datele cu caracter personal stocate, în conformitate cu principiile generale ale RGPD (vezi *secțiunea 8*).

103. În ceea ce privește supravegherea video, trebuie menționat că, de exemplu, prin estomparea imaginii fără capacitatea retroactivă de a recupera datele cu caracter personal pe care le-a conținut anterior, datele cu caracter personal sunt considerate șterse în conformitate cu RGPD.

> Exemplu: Un magazin de proximitate care are probleme cu vandalismul, în special la exterior, și, prin urmare, folosește supraveghere video pe partea exterioară a intrării, în legătură directă cu pereții. Un trecător solicită ca datele sale personale să fie șterse chiar din acel moment. Operatorul este obligat să răspundă cererii fără întârzieri nejustificate și în termen de cel mult o lună. Întrucât înregistrările în cauză nu mai îndeplinesc scopul pentru care au fost stocate inițial (nu a avut loc niciun act de vandalism în perioada în care persoana vizată a trecut prin zonă), la momentul solicitării nu există niciun interes legitim de a stoca datele care să prevaleze asupra intereselor persoanelor vizate. Operatorul trebuie să șteargă datele cu caracter personal.

104.

6.2.2 Dreptul la opoziție

105. În cazul supravegherii video bazate pe *interesul legitim* [articolul 6 alineatul (1) litera (f) din RGPD] sau pe necesitatea de a îndeplini o sarcină care servește unui *interes public* [articolul 6 alineatul (1) litera (e) din RGPD], persoana vizată are dreptul – în orice moment – să se opună prelucrării, din motive legate de situația sa particulară, în conformitate cu articolul 21 din RGPD. Cu excepția cazului în care operatorul demonstrează motive legitime imperioase care prevalează asupra drepturilor și intereselor persoanei vizate, prelucrarea datelor persoanei care s-a opus trebuie să înceteze. Operatorul trebuie să fie obligat să răspundă cererilor persoanei vizate fără întârzieri nejustificate și în termen de cel mult o lună.

106. În contextul supravegherii video, această opoziție ar putea fi formulată la intrarea, în timpul petrecut în interior sau la părăsirea zonei monitorizate. În practică, acest lucru înseamnă că, exceptând cazul în care operatorul are motive legitime imperioase, monitorizarea unei zone în care persoanele fizice ar putea fi identificate este legală numai dacă:

(1) operatorul este capabil să oprească imediat camera de la prelucrarea datelor cu caracter personal la cerere, sau

(2) zona monitorizată este restricționată în detaliu, astfel încât operatorul poate asigura aprobarea persoanei vizate înainte de a intra în zonă și nu este o zonă la care persoana vizată ca cetățean are drept de acces.

107. Prezentul ghid nu își propune să identifice ce se consideră a fi un interes legitim *imperios* (articolul 21 din RGPD).

108. Atunci când se utilizează supravegherea video în scopul marketingului direct, persoana vizată are dreptul să se opună prelucrării în mod discreționar, întrucât dreptul de opoziție este absolut în acest context [articolul 21 alineatele (2) și (3) din RGPD].

> Exemplu: O companie întâmpină dificultăți constând în încălcări ale securității la intrarea publică și folosește supraveghere video pe motive de interes legitim, cu scopul de a-i surprinde pe cei care intră ilegal. Un vizitator se opune prelucrării datelor sale prin sistemul de supraveghere video din motive legate de situația sa particulară. Totuși, în acest caz, compania respinge cererea explicând că înregistrările stocate sunt necesare pentru o anchetă internă aflată în curs, având astfel motive legitime imperioase pentru a continua prelucrarea datelor cu caracter personal.

109.

7 OBLIGAȚII PRIVIND TRANSPARENȚA ȘI INFORMAREA[18]

110. De mult timp este inerentă, în legislația europeană privind protecția datelor, ideea că persoanele vizate trebuie să fie conștiente de faptul că supravegherea video este în funcțiune. Persoanele vizate trebuie informate în detaliu cu privire la locurile monitorizate[19]. Potrivit RGPD, obligațiile generale privind transparența și informarea sunt stabilite la articolul 12 și următoarele. Ghidul privind transparența conform Regulamentului 2016/679 (WP 260) al Grupului de Lucru instituit prin articolul 29, care a fost avizat de CEPD la 25 mai 2018, oferă detalii suplimentare. În conformitate cu WP 260 punctul 26, articolul 13 din RGPD este cel care se aplică dacă datele cu caracter personal sunt culese „[…] de la o persoană vizată prin observare (de exemplu, folosind dispozitive automate de captare a datelor sau software de captare a datelor, cum ar fi camere de luat vederi […]".

111. Având în vedere volumul informațiilor care trebuie furnizate persoanei vizate, operatorii de date pot adopta o abordare pe mai multe niveluri atunci când optează pentru utilizarea unei combinații de metode pentru asigurarea transparenței (WP 260, punctul 35; WP 89, punctul 22). În ceea ce privește supravegherea video, cele mai importante informații trebuie afișate pe semnul de avertizare (primul nivel), în timp ce alte detalii obligatorii pot fi furnizate prin alte mijloace (al doilea nivel).

7.1 Informații din primul nivel (mesajul de avertizare)

112. Primul nivel se referă la principalul mod în care operatorul comunică pentru prima dată cu persoana vizată. În acest stadiu, operatorii pot utiliza un mesaj de avertizare care să conțină informații relevante. Informațiile afișate pot fi furnizate în combinație cu o pictogramă pentru a oferi într-un mod ușor vizibil, inteligibil și clar lizibil o imagine de ansamblu semnificativă asupra prelucrării avute în vedere [articolul 12 alineatul (7) din RGPD]. Formatul informării trebuie ajustat în funcție de amplasamentul acesteia (WP 89, punctul 22).

7.1.1 Poziționarea mesajului de avertizare

113. Informațiile trebuie poziționate astfel încât persoana vizată să poată recunoaște cu ușurință circumstanțele supravegherii înainte de a intra în zona monitorizată (aproximativ la nivelul ochilor). Nu este necesar să se divulge poziția camerei, atâta timp cât nu există niciun dubiu asupra zonelor supuse monitorizării, iar contextul supravegherii este clarificat fără ambiguitate (WP 89, punctul 22). Persoana vizată trebuie să poată estima zona captată de o cameră de luat vederi, ca să poată evita supravegherea sau să-și adapteze comportamentul, dacă este necesar.

7.1.2 Conținutul primului nivel

114. Informațiile din primul nivel (mesajul de avertizare) trebuie să transmită în general cele mai importante detalii, de exemplu detalii despre scopurile prelucrării, identitatea operatorului și existența drepturilor persoanei vizate, împreună cu detalii despre cele mai importante efecte ale prelucrării[20]. Mesajul poate cuprinde, de exemplu, interesele legitime urmărite de operator (sau

[18] Este posibil să se aplice cerințe specifice din legislația națională.

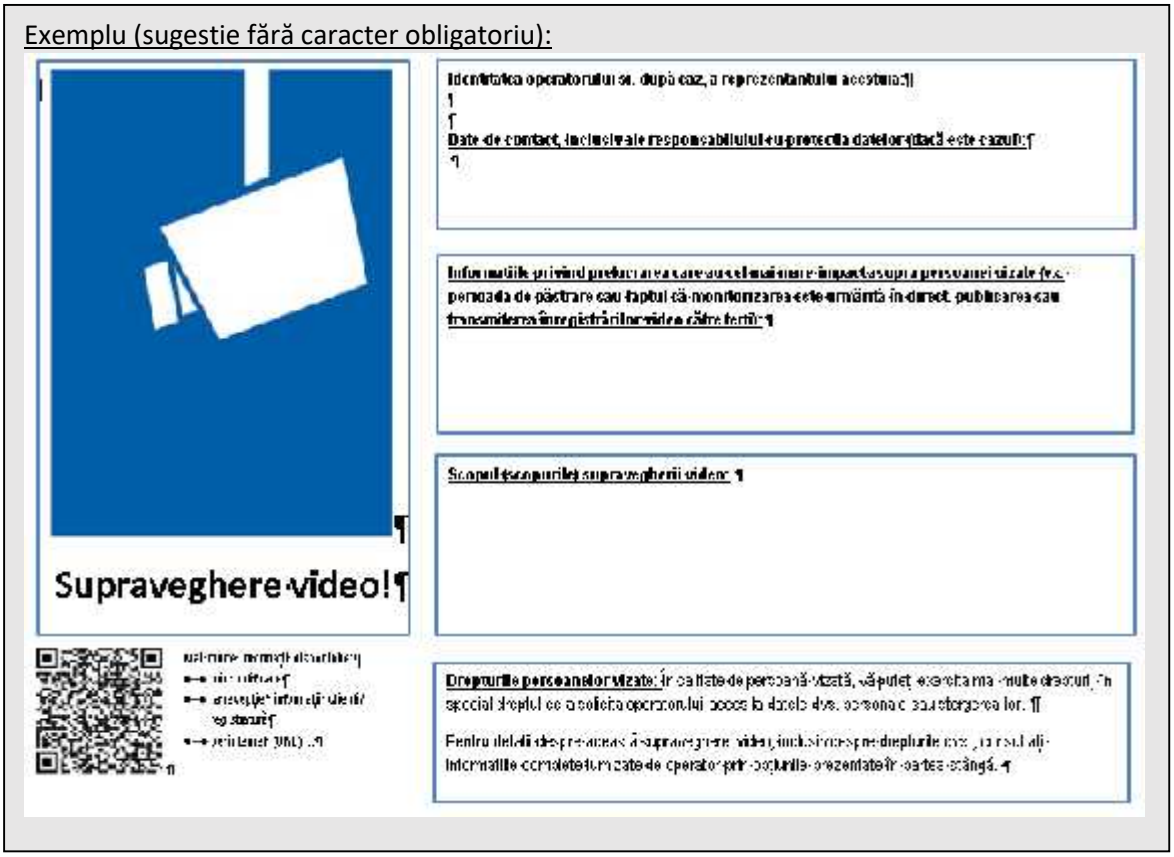
[19] Vezi WP 89, Avizul 4/2004 privind prelucrarea datelor cu caracter personal prin mijloace de supraveghere video al Grupului de lucru instituit prin articolul 29).

[20] Vezi WP 260, punctul 38.

de către o parte terță) și informațiile de contact ale responsabilului cu protecția datelor (dacă este cazul). De asemenea, mesajul trebuie să facă referire la cel de-al doilea nivel, mai detaliat, de informații și la locul și modul în care poate fi găsit.

115. În plus, mesajul trebuie să conțină și orice fel de informație care ar putea surprinde persoana vizată (WP 260, punctul 38). Ar putea fi vorba, de exemplu, despre transmiteri către părți terțe, în special dacă acestea sunt situate în afara UE, și despre perioada de stocare. Dacă aceste informații nu sunt precizate, persoana vizată trebuie să poată avea încredere că este doar o monitorizare live (fără înregistrări sau transmiteri de date către părți terțe).

116. Exemplu (sugestie fără caracter obligatoriu):



7.2 Informații din cel de-al doilea nivel

117. Și informațiile din cel de-al doilea nivel trebuie furnizate persoanei vizate într-un loc ușor accesibil, de exemplu sub forma unei fișe cu informații complete disponibilă într-un loc central (de exemplu, birou de informații, recepție sau casierie) sau afișate pe un panou ușor accesibil. Așa cum s-a menționat mai sus, mesajul de avertizare din primul nivel trebuie să facă o referire clară la informațiile de la doilea nivel. În plus, cel mai bine este dacă informațiile din primul nivel fac referire la o sursă digitală (de exemplu, codul QR sau o adresă a unui site) a celui de-al doilea nivel. Însă informațiile trebuie să fie ușor accesibile și în format non-digital. Informațiile din cel de-al doilea nivel trebuie să poată fi accesate fără a intra în zona supravegheată, în special dacă informațiile sunt furnizate digital (acest lucru se poate realiza, de exemplu, printr-un link). Alte mijloace adecvate ar putea consta într-un număr de telefon care să poată fi apelat. Indiferent de modul în care sunt furnizate, informațiile trebuie să conțină tot ce este obligatoriu în conformitate cu articolul 13 din RGPD.

118. Pe lângă aceste opțiuni și, de asemenea, pentru a le face mai eficiente, CEPD promovează utilizarea mijloacelor tehnologice pentru a furniza informații persoanelor vizate. Aici pot fi

incluse, de exemplu, camerele de geolocalizare și introducerea informațiilor în aplicații de cartografiere sau site-uri, pentru ca persoanele să poată identifica cu ușurință și să poată specifica sursele video care au legătură cu exercitarea drepturilor lor pe de o parte, iar pe de altă parte, să obțină informații mai detaliate despre operațiunea de prelucrare.

Exemplu: Proprietarul unui magazin își monitorizează magazinul. Pentru a respecta articolul 13 este suficient să amplaseze un mesaj de avertizare, care să conțină informațiile din primul nivel, într-un punct ușor vizibil la intrarea în magazin. În plus, trebuie să afișeze o fișă cu informații care să conțină informațiile din al doilea nivel la casierie sau în alt loc central și ușor accesibil din magazin.

119.

8 PERIOADELE DE STOCARE ȘI OBLIGAȚIA DE ȘTERGERE

120. Datele cu caracter personal nu pot fi stocate pe o perioadă care depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele cu caracter personal [articolul 5 alineatul (1) literele (c) și (e) din RGPD]. În unele state membre, pot exista dispoziții specifice pentru perioadele de stocare cu privire la supravegherea video în conformitate cu articolul 6 alineatul (2) din RGPD.

121. Trebuie verificat într-un interval scurt dacă este necesar ca datele cu caracter personal să fie stocate. În general, scopurile legitime pentru supravegherea video sunt adesea protejarea proprietății sau păstrarea dovezilor. De obicei, daunele produse pot fi recunoscute în termen de una sau două zile. Pentru a facilita demonstrarea conformității cu cadrul de protecție a datelor, este în interesul operatorului să facă aranjamente organizatorice în prealabil (de exemplu, să desemneze, dacă este necesar, un reprezentant pentru vizualizarea și securizarea materialului video). Având în vedere principiile prevăzute la articolul 5 alineatul (1) literele (c) și (e) din RGPD, și anume reducerea la minimum a datelor și limitările legate de stocare, datele cu caracter personal trebuie șterse în mod ideal automat, după câteva zile, în majoritatea cazurilor (de exemplu, în scopul depistării actelor de vandalism). Cu cât perioada de stocare stabilită este mai lungă (mai ales când depășește 72 de ore), cu atât este nevoie de o argumentare mai solidă pentru legitimitatea scopului și necesitatea stocării. Dacă operatorul folosește supravegherea video nu numai pentru monitorizarea spațiilor sale, ci și cu intenția de a stoca datele, trebuie să se asigure că stocarea este într-adevăr necesară pentru îndeplinirea scopului. În caz afirmativ, perioada de stocare trebuie să fie definită clar și stabilită individual pentru fiecare scop în cauză. Operatorului îi revine responsabilitatea de a defini perioada de păstrare în conformitate cu principiul necesității și al proporționalității și de a demonstra respectarea dispozițiilor RGPD.

> Exemplu: Proprietarul unui magazin mic ar observa, în mod normal, un act de vandalism în aceeași zi în care a avut loc. În consecință, este suficientă o perioadă de stocare obișnuită de 24 de ore. Însă zilele de weekend în care nu se lucrează sau vacanțele prelungite pot justifica o perioadă de stocare mai lungă. Dacă se constată o pagubă, poate fi necesar să se păstreze înregistrările video pentru o perioadă mai lungă pentru a se lua măsuri legale împotriva infractorului.

122.

9 MĂSURI TEHNICE ȘI ORGANIZATORICE

123. Astfel cum se prevede la articolul 32 alineatul (1) din RGPD, prelucrarea datelor cu caracter personal în timpul supravegherii video nu trebuie să fie doar permisă din punct de vedere legal, ci și securizată corespunzător de către operatori și persoanele împuternicite de aceștia. **Măsurile organizatorice și tehnice** puse în aplicare trebuie să fie **proporționale cu riscurile la adresa drepturilor și libertăților persoanelor fizice** care sunt generate, în mod accidental sau ilegal, din distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele obținute prin supraveghere video. Conform articolelor 24 și 25 din RGPD, operatorii trebuie să pună în aplicare măsuri tehnice și organizatorice inclusiv pentru a garanta toate principiile de protecție a datelor în timpul prelucrării, precum și să stabilească mijloace prin care persoanele vizate să-și exercite drepturile definite la articolele 15-22 din RGPD. Operatorii de date trebuie să

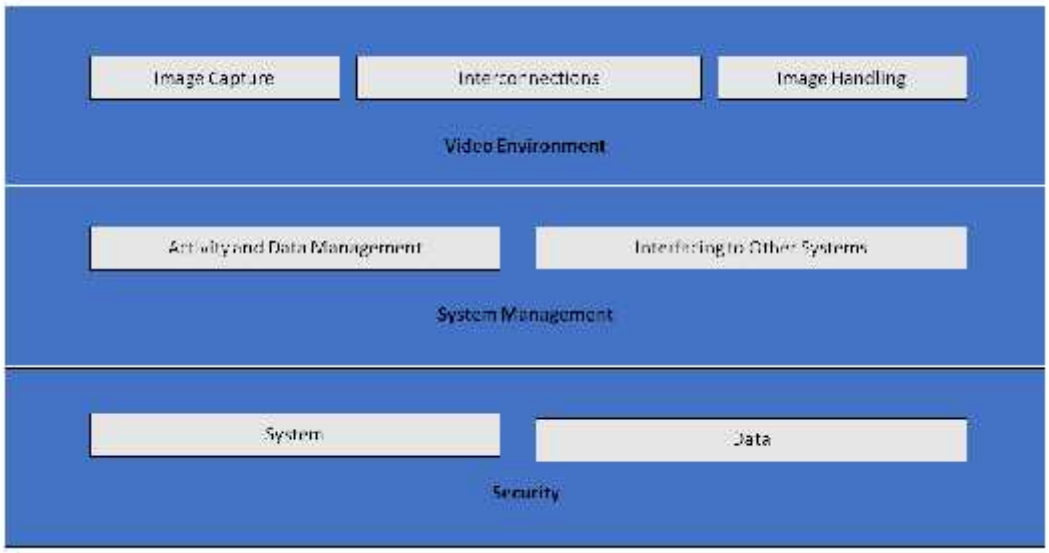
adopte cadrul și politicile interne care să asigure această punere în aplicare atât la momentul stabilirii mijloacelor de prelucrare, cât și la momentul prelucrării în sine, inclusiv prin efectuarea de evaluări ale impactului asupra protecției datelor dacă este necesar.

9.1 Prezentare generală a sistemului de supraveghere video

124. Un sistem de supraveghere video (SSV)[21] este alcătuit din dispozitive analogice și digitale, precum și din software pentru captarea imaginilor unei scene, prelucrarea imaginilor și afișarea lor unui operator. Componentele sale sunt grupate în următoarele categorii:

- Mediul video: captarea imaginilor, interconectări și prelucrarea imaginilor:
  - scopul captării imaginilor este generarea unei imagini a lumii reale într-un format în care să poată fi utilizată de restul sistemului,
  - interconectările descriu toate transmisiile de date din mediul video, mai precis conectările și comunicațiile. Cablurile, rețelele digitale și transmisiile wireless reprezintă exemple de conectări. Comunicațiile descriu toate semnalele video și de date de control, care pot fi digitale sau analogice,
  - prelucrarea imaginilor se referă la analiza, stocarea și prezentarea unei imagini sau a unei secvențe de imagini.
- Din perspectiva gestionării sistemului, un SSV are următoarele funcții logice:
  - gestionarea datelor și a activităților, care include procesarea comenzilor operatorilor și a activităților generate de sistem (proceduri de alarmă, alertarea operatorilor),
  - interfețe cu alte sisteme, printre care conectarea la alte sisteme de securitate (controlul accesului, alarmă de incendiu) și fără legătură cu securitatea (sisteme de gestionare a clădirilor, recunoaștere automată a numărului de înmatriculare).
- Securitatea SSV constă în confidențialitatea, integritatea și disponibilitatea sistemului și a datelor:
  - securitatea sistemului presupune securitatea fizică a tuturor componentelor sistemului și controlul accesului la SSV,
  - securitatea datelor se referă la prevenirea pierderii sau a manipulării datelor.

[21] RGPD nu oferă o definiție; se poate găsi o descriere tehnică, de exemplu, în standardul EN 62676-1-1:2014 Sisteme de supraveghere video pentru aplicații de securitate – partea 1-1: Cerințele sistemelor video.



125.

Image Capture	Captarea imaginilor
Interconnections	Interconectări
Image Handling	Prelucrarea imaginilor
Video Environment	Mediul video
Activity and Data Management	Gestionarea activităților și a datelor
Interfacing to Other Systems	Interfața cu alte sisteme
System Management	Gestionarea sistemului
System	Sistemul
Data	Datele
Security	Securitatea

Figura 1 – Sistemul de supraveghere video

9.2 Asigurarea protecției datelor începând cu momentul conceperii și în mod implicit

126. După cum se precizează la articolul 25 din RGPD, operatorii trebuie să pună în aplicare măsuri tehnice și organizatorice adecvate de protecție a datelor din momentul în care începe să planifice supravegherea video – înainte de a începe să adune și să prelucreze material video. Aceste principii evidențiază necesitatea unor tehnologii integrate de îmbunătățire a confidențialității, a unor setări implicite care să reducă la minimum prelucrarea datelor și a furnizării instrumentelor necesare care să permită cea mai mare protecție posibilă a datelor cu caracter personal[22].

127. Operatorii trebuie să includă garanții pentru protecția datelor și a vieții private nu numai în specificațiile de proiectare a tehnologiei, ci și în practicile organizaționale. În ceea ce privește practicile organizaționale, operatorul trebuie să adopte un cadru de gestionare adecvat, să stabilească și să aplice politici și proceduri referitoare la supravegherea video. Din punct de vedere tehnic, specificațiile și proiectarea sistemului trebuie să includă cerințe pentru prelucrarea datelor cu caracter personal în conformitate cu principiile enunțate la articolul 5 din RGPD [legalitatea prelucrării, limitări legate de scop și de stocarea datelor, reducerea la

[22] WP 168, Aviz privind „Viitorul vieții private", contribuție comună din partea Grupului de Lucru instituit prin articolul 29 și a Grupului de Lucru pentru poliție și justiție la Consultarea Comisiei Europene privind cadrul juridic pentru dreptul fundamental la protecția datelor cu caracter personal (adoptat la 1 decembrie 2009).

minimum a datelor în mod implicit în sensul articolului 25 alineatul (2) din RGPD, integritate și confidențialitate, responsabilitate etc.]. În cazul în care un operator intenționează să achiziționeze un sistem comercial de supraveghere video, trebuie să includă aceste cerințe în caietul de sarcini. Operatorul trebuie să asigure respectarea acestor cerințe aplicându-le pentru toate componentele sistemului și toate datele prelucrate de acesta, pe parcursul întregului lor ciclu de viață.

9.3 Exemple concrete de măsuri relevante

128. Majoritatea măsurilor care pot fi utilizate pentru a asigura supravegherea video, în special atunci când sunt utilizate echipamente digitale și software, nu diferă de cele utilizate în alte sisteme informatice. Totuși, indiferent de soluția selectată, operatorul trebuie să protejeze în mod corespunzător toate datele și componentele sistemului de supraveghere video în toate etapele, adică pe durata stocării (date în repaus), al transmisiei (date în tranzit) și al prelucrării (date în uz). Pentru aceasta, este necesar ca operatorii și persoanele împuternicite de ei să aplice o combinație de măsuri organizatorice și măsuri tehnice.

129. Atunci când selectează soluțiile tehnice, operatorul trebuie să ia în considerare și tehnologii favorabile confidențialității, deoarece îmbunătățesc securitatea. Câteva exemple de astfel de tehnologii sunt sistemele care permit mascarea sau distorsionarea zonelor irelevante pentru supraveghere sau eliminarea din înregistrare a imaginii persoanelor terțe atunci când înregistrările video se pun la dispoziția persoanelor vizate[23]. Pe de altă parte, soluțiile selectate nu trebuie să ofere funcții care nu sunt necesare (de exemplu, mișcare nelimitată a camerelor, capacitate de mărire, transmisie radio, analiză și înregistrări audio). Funcțiile care sunt oferite, dar nu sunt necesare, trebuie dezactivate.

130. Există o bogată literatură de specialitate disponibilă pe această temă, inclusiv standarde internaționale și specificații tehnice privind securitatea fizică a sistemelor multimedia[24] și securitatea sistemelor informatice generale[25]. Prin urmare, secțiunea de față oferă doar o imagine de ansamblu, în linii mari, a acestui subiect.

9.3.1 Măsuri organizatorice

131. Pe lângă necesitatea unei potențiale evaluări a impactului asupra protecției datelor (EIPD) (vezi *secțiunea 10*), operatorii trebuie să ia în considerare următoarele subiecte atunci când își formulează propriile politici și proceduri privind supravegherea video:

- cine răspunde de gestionarea și funcționarea sistemului de supraveghere video;
- scopul și sfera de cuprindere a proiectului de supraveghere video;
- utilizarea adecvată și cea interzisă (unde și când este permisă supravegherea video, unde și când nu este permisă; de exemplu, utilizarea de camere ascunse și înregistrarea audio, în plus față de înregistrarea video)[26];

[23] Utilizarea unor astfel de tehnologii poate fi chiar obligatorie în unele cazuri, în scopul respectării articolului 5 alineatul (1) litera (c). În orice caz, ele pot servi drept exemple de bune practici.

[24] IEC TS 62045 — Securitate multimedia – Ghid pentru protecția vieții private în cazul echipamentelor și sistemelor aflate sau ieșite din uz.

[25] ISO/IEC 27000 — Serie privind sistemele de management al securității informației.

[26] Aceasta poate depinde de legislația națională și de reglementările sectoriale.

- măsurile privind transparența menționate în *secțiunea 7 (Obligații privind transparența și informarea)*;
- modul de înregistrare și durata materialului video, inclusiv stocarea în arhive a înregistrărilor video referitoare la incidente de securitate;
- cine trebuie să beneficieze de instruire tematică și când;
- cine are acces la înregistrările video și în ce scopuri;
- procedurile operaționale (de exemplu, de către cine și de unde este monitorizată supravegherea video, ce trebuie făcut în cazul unui incident de încălcare a securității datelor);
- procedurile pe care trebuie să le urmeze părțile externe pentru a solicita înregistrări video și procedurile pentru respingerea sau aprobarea acestor cereri;
- procedurile de achiziție, instalare și întreținere a SSV;
- procedurile de gestionare a incidentelor și de recuperare a datelor.

9.3.2 Măsuri tehnice

132. **Securitatea sistemului** înseamnă **securitatea fizică** a tuturor componentelor sistemului și integritatea sistemului, adică **protecția împotriva interferențelor intenționate și neintenționate în funcționarea sa obișnuită și reziliența față de acestea**, precum și **controlul accesului**. Securitatea datelor înseamnă **confidențialitate** (datele sunt accesibile doar persoanelor cărora li s-a acordat acces), **integritate** (prevenirea pierderilor de date sau a manipulării datelor) și **disponibilitate** (datele pot fi accesate atunci când este necesar).

133. **Securitatea fizică** este o parte esențială a protecției datelor și prima linie de apărare, deoarece protejează echipamentele SSV de furt, vandalism, catastrofe naturale, catastrofe provocate de om și daune accidentale (de exemplu, supratensiuni electrice, temperaturi extreme și cafea vărsată). În cazul sistemelor de tip analog, securitatea fizică are rol principal în protecția lor.

134. **Securitatea sistemului și a datelor**, adică protecția împotriva interferențelor intenționate și neintenționate în funcționarea sa obișnuită, poate include:

- protecția întregii infrastructuri SSV (inclusiv camerele de la distanță, cablarea și alimentarea cu energie electrică) împotriva manipulării fizice frauduloase și a furtului fizic;
- protecția transmiterii înregistrărilor împotriva interceptării prin canale de comunicare sigure;
- criptarea datelor;
- utilizarea de soluții bazate pe hardware și software, cum ar fi sisteme firewall, antivirus sau de detectare a intruziunilor împotriva atacurilor cibernetice;
- detectarea disfuncționalităților la nivel de componente, software și interconectări;
- mijloace de restabilire a disponibilității și a accesului la sistem în cazul unui incident fizic sau tehnic.

135. **Controlul accesului** înseamnă că numai persoanele autorizate pot accesa sistemul și datele, iar celelalte nu pot avea acces. Măsurile care sprijină controlul accesului fizic și logic cuprind:

- garantarea faptului că toate spațiile în care se realizează monitorizarea prin supraveghere video și în care sunt stocate înregistrările video sunt asigurate împotriva accesului nesupravegheat al terților;
- poziționarea monitoarelor (mai ales când se află în zone deschise, cum ar fi o recepție) astfel încât numai operatorii autorizați să le poată vizualiza;
- definirea și aplicarea de proceduri de acordare, schimbare și revocare a accesului fizic și logic;

- punerea în aplicare de metode și mijloace de autentificare și autorizare a utilizatorilor, inclusiv, de exemplu, lungimea parolelor și frecvența schimbării acestora;
- înregistrarea și analiza periodică a acțiunilor efectuate de utilizatori (atât la nivel de sistem, cât și în ceea ce privește datele);
- monitorizarea și detectarea tentativelor nereușite de acces se desfășoară permanent, iar punctele slabe sunt identificate cât mai curând.

10 EVALUAREA IMPACTULUI ASUPRA PROTECȚIEI DATELOR

136. Conform articolului 35 alineatul (1) din RGPD, operatorii au obligația de a efectua evaluări ale impactului asupra protecției datelor (EIPD) atunci când un tip de prelucrare a datelor este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice. Articolul 35 alineatul (3) litera (c) din RGPD prevede că operatorii au obligația de a efectua evaluări ale impactului asupra protecției datelor dacă prelucrarea constituie o monitorizare sistematică pe scară largă a unei zone accesibile publicului. În plus, în conformitate cu articolul 35 alineatul (3) litera (b) din RGPD, o evaluare a impactului asupra protecției datelor se impune, de asemenea, atunci când operatorul intenționează să prelucreze pe scară largă categorii speciale de date.

137. Ghidul privind evaluarea impactului asupra protecției datelor[27] oferă recomandări suplimentare și exemple mai detaliate relevante pentru supravegherea video (de exemplu, cu privire la „utilizarea unui sistem de camere pentru monitorizarea comportamentului conducătorilor auto pe autostrăzi"). Articolul 35 alineatul (4) din RGPD prevede ca fiecare autoritate de supraveghere să publice o listă a tipurilor de operațiuni de prelucrare care fac obiectul obligației de a efectua o DPIA în țara respectivă. Aceste liste pot fi găsite de obicei pe site-urile autorităților. Având în vedere scopurile obișnuite ale supravegherii video (protecția persoanelor și a bunurilor, depistarea, prevenirea și controlul infracțiunilor, colectarea de dovezi și identificarea biometrică a suspecților), este rezonabil să se presupună că EIPD va fi necesară în multe cazuri de supraveghere video. Prin urmare, operatorii de date trebuie să consulte cu atenție aceste documente pentru a stabili dacă este necesară o astfel de evaluare și să o efectueze dacă este necesară. Rezultatul EIPD efectuate trebuie să sprijine operatorul în alegerea sa cu privire la măsurile de protecție a datelor pe care le va pune în aplicare.

138. De asemenea, este important de menționat că, în cazul în care rezultatele EIPD indică faptul că prelucrarea ar genera un risc mare în pofida măsurilor de securitate prevăzute de operator, atunci va trebui consultată autoritatea de supraveghere relevantă înainte de prelucrare. Detalii despre consultările anterioare pot fi găsite la articolul 36.

Pentru Comitetul European pentru Protecția Datelor

Președintele

(Andrea Jelinek)

[27] WP 248 rev. 01, Ghid privind evaluarea impactului asupra protecției datelor (EIPD), care stabilește dacă prelucrarea este „susceptibilă să genereze un risc ridicat" în sensul Regulamentului 2016/679 - aprobat de CEPD.