Considerente în legătură cu utilizarea tot mai frecventă a sistemului de supraveghere video înzestrat cu funcții de înregistrare audio

Potrivit prevederilor Legii nr. 175/2021 pentru modificarea unor acte normative *a fost exclusă obligația operatorului de a notifica Centrul National pentru Protecția Datelor cu Caracter Personal al Republicii Moldova (CNPDCP) operațiunile de prelucrare a datelor cu caracter personal*, precum și *a fost instituită obligația operatorului de a efectua evaluarea impactului asupra protecției datelor cu caracter personal, în cazul în care prelucrarea datelor poate genera un risc sporit pentru drepturile și libertățile persoanelor, inclusiv de a desemna o persoană responsabilă cu protecția datelor cu caracter personal*.

Consecvent, Legea nr. 133/2011 privind protecția datelor cu caracter personal (în continuare – Legea nr. 133/2011) prevede, în art. 1, că *scopul acesteia este asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieţii intime, familiale şi private.*

În continuare, se relevă că, deținerea și utilizarea mijloacelor video și/sau prelucrarea datelor personale prin intermediul acestora trebuie să fie compatibilă și adecvată sarcinilor și atribuțiilor operatorului și poate avea loc doar în scopul asigurării securității persoanelor şi bunurilor, pazei şi protecţiei bunurilor, imobilelor, valorilor şi a materialelor cu regim special, respectând în acelaşi timp obligaţiile ce revin entității, în calitate de operator, conform legii prenotate și măsurile de securitate adoptate pentru protecţia datelor cu caracter personal, protejarea vieţii private, a intereselor legitime şi garantarea drepturilor fundamentale ale persoanelor vizate.

Pe aceeași dimensiune de abordare, atragem atenția asupra faptului că, prin montarea sistemului de evidență supraveghere video care ar putea colecta vocea (înregistrarea audio) va fi afectat dreptul la viața privată a salariaților și vizitatorilor operatorilor de date cu caracter personal sau a altor persoane care nimeresc în raza de captare a acestora din următoarele considerente:

a. Potrivit art. 12 din Declarația Universală a Drepturilor Omului și art. 17 din Pactul internațional cu privire la drepturile civile și politice, *nimeni nu va fi obiectul unor imixtiuni arbitrare în viața sa particulară, în familia sa, în domiciliul său ori în corespondență, nici al unor atingeri ale onoarei sau reputației sale. Orice persoană are dreptul la protecţia legii împotriva unor astfel de imixtiuni sau atingeri*.

b. Art. 8 din Convenția pentru apărarea drepturilor omului şi a libertăţilor fundamentale (în continuare – CoEDO) statuează că, *orice persoană are dreptul la respectarea vieţii sale private şi de familie, a domiciliului său şi a corespondenţei sale*.

c. Art. 7 din Carta Drepturilor Fundamentale a Uniunii Europene reglementează respectarea vieții private și intime. Totodată, art. 8 din Cartă prevede că, *orice persoană are dreptul la protecția datelor cu caracter personal care o privesc. Asemenea date trebuie tratate în mod corect, în scopurile precizate şi pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege*.

d. Convenția Consiliului Europei pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (în continuare – Convenția nr. 108) se aplică tuturor cazurilor de prelucrare a datelor în sectoarele public și privat și protejează persoana, împotriva abuzurilor care pot însoți prelucrarea datelor cu caracter personal.

e. În continuare, considerentul nr. 84 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27.04.2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal şi privind libera circulație a acestor date şi de abrogare a Directivei 95/46/CE (în continuare – RGPD) prevede că, [... *în cazul în care operațiunile de prelucrare a datelor cu caracter personal sunt susceptibile să genereze un risc ridicat pentru drepturile şi libertățile persoanelor fizice, operatorul ar trebui să fie responsabil de efectuarea unei evaluări a impactului asupra protecției datelor, care să estimeze, în special, originea, natura, specificitatea și gravitatea acestui risc* ...].

f. Suplimentar, facem referire la următoarele raționamente menționate în **Avizul nr. 2/2017 privind prelucrarea datelor la locul de muncă,** *adoptat la 08.05.2017 de către Grupul de lucru Art. 29 privind protecția datelor* (disponibil pe Internet la adresa: https://ec.europa.eu/newsroom/article29/items/610169/en), potrivit cărora, „*tehnologiile moderne permit angajaților să fie urmăriți în timp, de la un loc de muncă la altul și în locuințele lor prin intermediul a numeroase dispozitive diferite cum ar fi telefoanele inteligente, calculatoarele de birou, tabletele, vehiculele şi dispozitivele destinate purtării. În cazul în care nu există limite cu privire la prelucrare și, în cazul în care aceasta (prelucrarea) nu este transparentă, există un risc ridicat ca interesul legitim al angajatorilor în îmbunătățirea eficienței și protecția activelor societăților să se transforme într-o acțiune de monitorizare nejustificată și intruzivă. [...] În plus, datorită capacităților unor astfel de tehnologii, este posibil ca angajații să nu știe ce date cu caracter personal sunt prelucrate și în ce scopuri, în același timp fiind posibil, de asemenea, ca aceștia să nu știe nici măcar de existența însăși a tehnologiei de monitorizare*".

g. **Pct. 129 din Ghidul nr. 3/2019 privind prelucrarea datelor prin mijloace de supraveghere video**, aprobat în cadrul Plenarei Comitetului European pentru Protecția Datelor (*disponibil pe Internet la adresa:* https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en) stipulează că, „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. 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**".

h. Art. 28 din **Constituția Republicii Moldova** prevede că, *statul respectă și ocrotește viața intimă, familială și privată*. Totodată, art. 54 alin. (2) și (4) din **Constituția Republicii Moldova**, statuează că, *exercițiul drepturilor şi libertăților nu poate fi supus altor restrângeri decât celor prevăzute de lege, care corespund normelor unanim*

recunoscute ale dreptului internaţional şi sunt necesare în interesele securităţii naţionale, integrităţii teritoriale, bunăstării economice a ţării, ordinii publice, în scopul prevenirii tulburărilor în masă şi infracţiunilor, protejării drepturilor, libertăţilor şi demnităţii altor persoane, împiedicării divulgării informaţiilor confidenţiale sau garantării autorităţii şi imparţialităţii justiţiei. Restrângerea trebuie să fie proporţională cu situaţia care a determinat-o şi nu poate atinge existenţa dreptului sau a libertăţii.

i. Consecvent, subliniem că, operatorul are obligația să respecte și să asigure implementarea prevederilor art. art. 4, 5, 23 - 25, 29 alin. (1) și 30 alin. (1) din Legea nr. 133/2011. Reieșind din dispozițiile menționate supra, prelucrarea categoriei de date cu caracter personal precum **vocea (înregistrarea audio)** prin intermediul unui sistem de evidență supraveghere video și utilizarea dispozitivelor portative/mobile de către operator sunt excesive față de scopurile prelucrării datelor cu caracter personal, **din considerentul că, reprezintă o mai mare intruziune în viața privată a persoanelor monitorizate, şi anume, a angajaților și vizitatorilor entității publice și/sau private, care presupune documentarea înregistrată și reproductibilă a conduitei angajaților la locul de muncă şi/sau a vizitatorilor**.

j. În acest context subliniem că, jurisprudența Curții Europene a Drepturilor Omului (în continuare – Curtea) a examinat numeroase situații în care au apărut aspecte legate de protecția datelor prin prisma supravegherii video:

- În *cauza Niemietz c. Germania din 16.12.1992* (*disponibil pe Internet la adresa: https://www.echr.coe.int/Documents/FS_Workplace_surveillance_RON.pdf.)*, Curtea a considerat că, art. 8 din CoEDO oferă protecția unei persoane nu doar în cercul său intim, ci și în timpul și parcursul activității sale profesionale;
- În *cauza S. și M. Marper c. Regatului Unit din 04.12.2008 (disponibil pe Internet la adresa: https://www.echr.coe.int/Documents/FS_Workplace_surveillance_RON.pdf)*, Curtea a constatat că ingerința în respectarea dreptului la viața privată trebuie să fie proporțională cu scopul prelucrării datelor cu caracter personal;
- În *cauza Antović și Mirković vs. Muntenegru din 28.11.2017 (disponibil pe Internet la adresa: https://www.echr.coe.int/Documents/FS_Workplace_surveillance_RON.pdf)*, Curtea a hotărât că „supravegherea video la locul de muncă reprezintă o atingere adusă vieții private a angajatului (profesorului), deoarece amfiteatrele universitare sunt locurile de desfășurare a activității profesorilor, unde nu numai că aceștia predau, dar și interacționează cu studenții, stabilind relații și zidindu-și identitatea lor socială";
- În *cauza Allan c. Regatul Unit din 05.11.2002 (Disponibil pe Internet la adresa: https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001140543&filename=CASE%20OF%20 ALLEN%20v.%20THE%20UNITED20KINGDOM%20-%20%5BRomanian%20Translation%5D%20by%20the%20COE%20Human%20Rights%20 Trust%20Fund.pdf&logEvent=False)* - Întrucât, la momentul respectiv, nu exista niciun sistem legal de reglementare a utilizării de către poliție a dispozitivelor de înregistrare secrete, ingerința respectivă nu a fost în conformitate cu legea. Curtea a

constatat că utilizarea de dispozitive de înregistrare audio și video în celula reclamantului, în zona de vizită a penitenciarului și în apropierea unui alt deținut a adus atingere dreptului reclamantului la respectarea vieții private.

k. De asemenea, aducem în vizor și jurisprudența altor autorități de protecție a datelor cu caracter personal în domeniul prelucrării neconforme a datelor cu caracter personal prin intermediul mijloacelor de supraveghere video, cum ar fi:

- amenda administrativă de 72.000 de euro aplicată de către *Autoritatea Finlandeză pentru Protecția Datelor împotriva companiei „Taksi Helsinki Oy" (disponibil pe Internet la adresa: https://datepersonale.md/buletin-informativ-nr-5/)* pentru prelucrarea datelor cu caracter personal ale șoferilor, personalului și clienților șoferilor săi cu un sistem de supraveghere, care înregistrează atât video, cât și audio, care nu era în conformitate cu principiul RGPD de minimizare a datelor;
- amenda în mărime de 2.000 de euro aplicată de către *Autoritatea Suedeză pentru Protecția Datelor unei Asociații de Proprietari (disponibil pe Internet la adresa: https://datepersonale.md/amenda-de-2-mii-de-euro-aplicata-de-catre-autoritatea-suedeza-pentru-protectia-datelor-pentru-supravegherea-video-si-audio/)* care a amplasat patru camere de filmat în bloc (una la intrarea principală în scara blocului, două în zona scărilor și una în zona de depozitare) ce prelucrau atât imagini, cât și sunete. Totodată, s-a reținut că, pentru captarea de imagini, prin înregistrarea sunetelor, este necesară demonstrarea unui motiv obiectiv care justifică o ingerință suplimentară în viața privată a persoanelor, prin prelucrarea de date cu caracter personal și prin monitorizare audio, nu doar video. Acest lucru înseamnă, că orice Asociație de Proprietari, dacă vrea pe lângă filmare, să înregistreze și sunete prin intermediul unei camere audio/video, trebuie să se asigure că există motive suplimentare justificative pentru acest lucru. Dacă obiectivele urmărite ar putea fi atinse doar prin captarea de imagini, atunci înregistrarea audio nu se justifică;
- *Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal din România* a aplicat două avertismente și două amenzi în valoare de 5.000 euro, companiei *Entirely Shipping & Trading S.R.L. (disponibil pe Internet la adresa: https://www.dataprotection.ro/?page=O_noua_sanctiune_pentru_incalcarea_RGPD_2020_3&lang=ro)*, pentru încălcarea dispozițiilor art. art. 5 alin. (1) lit. a), b), c) și e), 6, 7, 9, 12 și 13 din RGPD. În urma investigației, s-au constatat următoarele:

a) operatorul nu a făcut dovada unui interes legitim justificat în ceea ce privește sistemul de supraveghere video instalat la sediul său, care să prevaleze asupra intereselor sau drepturilor și libertăților fundamentale ale persoanelor vizate, nu a făcut dovada consultării sindicatului sau, după caz, a reprezentanților angajaților înainte de introducerea sistemelor de monitorizare, precum și nici a faptului că alte forme și modalități mai puțin intruzive pentru atingerea scopului urmărit de angajator nu și-au dovedit anterior eficiența;

b) operatorul nu a făcut dovada existenței unor politici adecvate de protecție a datelor și a implementării unor măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc;

c) prelucrarea datelor biometrice prin intermediul sistemului de control acces nu erau colectate în scopuri adecvate, relevante și limitate la ceea ce era necesar în raport cu scopurile în care erau prelucrate;

d) operatorul nu a efectuat o evaluare a impactului asupra protecției datelor.

l) Totodată, informăm că, CNPDCP a avut în examinare cazuri vizând legalitatea prelucrării datelor cu caracter personal prin intermediul sistemului de supraveghere video, efectuând și înregistrări audio. În context, în cadrul examinării unei petiții depuse de către un subiect de date, CNPDCP a emis decizie prin care s-a constatat încălcarea prevederilor art. 4 alin. (1) lit. a), b), c), art. 5 alin. (1) ale Legii nr. 133/2011, la prelucrarea datelor cu caracter personal ale petiționarului, în legătură cu colectarea/înregistrarea vocii persoanei vizate, fără consimțământul acesteia, prin intermediul camerei de supraveghere video, instalate pe un pilon electric, ce cuprindea atât proprietatea gestionarului sistemului de supraveghere video, cât și o porțiune din spațiul ce nu-i aparținea ultimului, fără a fi identificat scopul determinat, explicit și legitim, legătura de cauzalitate dintre scop și datele prelucrate ale petiționarului, proporționalitatea, corectitudinea și concordanța cu normele legale în domeniul protecției datelor cu caracter personal. Așadar, ținând cont de cele sus-indicate, Centrul a reținut că, înainte de instalarea unui sistem de supraveghere video, operatorul de date trebuie întotdeauna să examineze critic dacă această măsură este, în primul rând, adecvată pentru îndeplinirea obiectivului dorit și, în al doilea rând, proporțională și necesară pentru scopurile sale, în raport cu interesele sau drepturile și libertățile fundamentale ale subiectului de date. Prin urmare, înregistrarea audiovizuală de către operatorul de date în cauză, prin intermediul camerei de supraveghere video, fără consimțământul persoanei vizate, constituia o măsură excesivă și disproporționată în raport cu scopul declarat, la caz, asigurarea securității proprietății.

Astfel, reieșind din cele elucidate supra, menționăm că, **orice persoană fizică sau juridică, de drept public sau privat, este în drept să dețină și să utilizeze mijloace video, cu condiția întrunirii cerințelor prevăzute de legislația din domeniul protecției datelor cu caracter personal, și anume: asigurarea condițiilor de bază pentru prelucrarea datelor cu caracter personal; evaluarea impactului asupra protecției datelor cu caracter personal, în cazul în care prelucrarea datelor poate genera un risc sporit pentru drepturile și libertățile persoanelor; desemnarea persoanei responsabile cu protecția datelor cu caracter personal; realizarea drepturilor subiecților de date cu caracter personal; a măsurilor organizatorice și tehnice necesare pentru asigurarea confidențialității și securității datelor cu caracter personal**.

Pentru oricare alte informații suplimentare, pot fi contactate persoanele responsabile din Direcția prevenire, supraveghere și evidență din cadrul Direcției generale supraveghere și conformitate a CNPDCP la numărul de telefon 0-22 811-801/811-802 sau e-mail dpse@datepersonale.md.