8
ПРИВАТНОСТ И ПРАШАЊА ОД ОБЛАСТА НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

ПОВРЗАНИ СО УПОТРЕБАТА НА **ДРОНОВИ, СКРИЕНИ КАМЕРИ,** ЕЛЕКТРОНСКО **НАБЉУДУВАЊЕ** НА **ВРАБОТЕНИ**

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

CIP - Каталогизација во публикација
Национална и универзитетска библиотека “Св. Климент Охридски”, Скопје

342.738:621.39(497.7)(035)

УГРИНОВСКА, Нина
Водич - прашања за приватност и заштита на податоци во врска со користењето на беспилотни летала, камери кои се носат (скриени камери), електронско следење на вработените / автори на документот Нина Угриновска. - Скопје : Дирекција за заштита на личните податоци, 2018. -
26 стр. : илустр. ; 21 см

ISBN 978-608-4682-37-0

а) Право на приватност - Телекомуникации - Македонија - Водичи COBISS.MK-ID 108237834

ВОДИЧ - ПРАШАЊА ЗА ПРИВАТНОСТ И ЗАШТИТА НА ПОДАТОЦИ ВО ВРСКА СО КОРИСТЕЊЕТО НА БЕСПИЛОТНИ ЛЕТАЛА, КАМЕРИ КОИ СЕ НОСАТ (СКРИЕНИ КАМЕРИ), ЕЛЕКТРОНСКО СЛЕДЕЊЕ НА ВРАБОТЕНИТЕ

Издавач
Дирекција за заштита на личните податоци

Автори на документот
Нина Угриновска

Лектура
Дијана Ристова

Дизајн
Маја Димеска-Крпач

Печатење
Пропоинт

Тираж
50 примероци

Февруари, 2018

ЕУ за ТЕБЕ!

Овој документ е изработен во рамки на проектот „Поддршка за пристап до правото на заштита на личните податоци “EuropeAid 135668/IH/SER/МК, финансиран од Европската Унија преку ИПА ТАИБ 2012 програмата и спроведен од Vialto Consulting од Унгарија, во соработка со IPS Институт од Словенија и Националното тело за заштита на личните податоци и слобода на информации од Унгарија. Ставовите и мислењата наведени во овој прирачник во ниеден случај не ги изразуваат ставовите на Европската Унија.

Содржина

Листа на кратенки

Кратенка	Опис
ЕУ	Европска Унија
ГДПР	Општа регулатива за заштита на личните податоци
ДЗЛП	Дирекција за Заштита на личните податоци
UAV	беспилотни летала
RPAS	далечински пилотирани антенски системи
FAA	Федералната администрација за воздухопловство
ЕДПС	Европскиот супервизор за заштита на податоци
CCTV	Систем за видеонадзор
BWV	Видео што се носи на тело
ICAO	Меѓународна организација за цивилно воздухопловство
АЦВ	Агенција за цивилно воздухопловство
EASA	Европска агенција за воздухопловна безбедност
RPAS	Далечински управуван систем за летање
NGFW	Алатки за превенција на загуба на податоци
NGFW	Системи за заштитни ѕидови за идните генерации
UTM	системи за управување со унифицирани закани
BYOD	Донеси свој сопствен уред
ICO	Комесар за информации во Велика Британија
ПВЗП	проценка на влијанието врз заштитата на податоците
РГ 29	Работна група 29
WP55	Документ на РГ29
ГПС	Систем за глобало позиционирање

ВОВЕД

Денес во 21-виот век технологијата брзо се менува и се подобрува, така што ризиците и заканите треба да се управуваат на ист начин. Ова ја прави приватноста да биде многу тесно поврзана со технологијата, па дури и поголемата безбедност на ЛИИ (лични идентификувачки информации) зависи од технологијата и употребата на дигиталните уреди и апликации.

За да се постигне најдобрата безбедност за нашите лични информации, треба да ја следиме најдобрата практика за користење на технолошки системи и да бидеме постојано свесни и едуцирани за нови закани и како да ги избегнеме или да ги ублажиме.

Земајќи го предвид гореспоменатото, ЕУ воспостави и одобри ГДПР (Општа регулатива за заштита на податоци) да ги штити ЛИИ и да воведе глоби и казни за непочитување на регулативата. Исто така, трети земји имаат свои прописи за заштита на личните податоци.

Македонија прв пат воведе Закон за заштита на личните податоци во 2005 година и постојано го подобрува и дополнува. ДЗЛП во моментов е во процес на прилагодување на македонскиот закон за лични податоци со ГДПР. Понатаму ќе биде доставен на разгледување и одобрување.

Сите контролори и обработувачи мора да се усогласат со оваа легислатива и да спроведат организациски и технички мерки во системите што имаат лични податоци.

ДЗЛП постојано работи на свеста на поединците од една страна и свеста на контролорите и обработувачите, од друга страна.

Македонскиот закон за заштита на личните податоци се спроведува во земјата, а ДЗЛП постојано ја проверува и испитува усогласеноста со сите барања.

Ова упатство е дефинирано да им помогне на контролорите и обработувачите да ги разберат законските барања, новите технолошки трендови и да спроведат технички и организациски мерки кои се соодветни на нивниот контекст.

ЦЕЛ

Овој водич е поврзано со најдобрите практики и безбедносни мерки кои треба да се имплементираат и следат во секојдневните дејности за активности поврзани со лични податоци, како што се користење на најновите технолошки достигнувања во деловните процеси, јавни прашања и приватно користење на одредени достигнувања.

Документот е наменет за раководството на организацијата и персоналот задолжен за обезбедување на обработката на лични податоци, како и за мониторингот на вработените и обезбедување на усогласеност со законите и регулативите за заштита на податоците.

Се базира на општоприфатените добри практики во Управување со ризици за безбедност на информациите и Систем за управување со безбедноста на информациите.

УПОТРЕБА НА БЕСПИЛОТНИ ЛЕТАЛА

ШТО СЕ БЕСПИЛОТНИ ЛЕТАЛА (ДРОНОВИ)?

За војската, тие се UAV (беспилотни летала) или RPAS (далечински пилотирани антенски системи). Сепак, тие се повеќе познати како беспилотни летала (дронови). Беспилотни летала се користат во ситуации кога летот со екипаж се смета за премногу ризичен или тежок. Тие ги обезбедуваат војниците со 24-часовно „око на небото", седум дена во неделата.

Беспилотните летала (UAV), познати како дронови, повторно ги „оживуваат" старите бизниси, па дури и создаваат сосема нови можности. Без разлика дали тоа е иновација во медиумското покривање и снимање на филмови или нови способности за одговорни лица за итни случаи, беспилотните летала се способни за некои прилично неверојатни нешта. Минатата година, Федералната администрација за воздухопловство (FAA) објави правила за комерцијална употреба на беспилотни летала, појаснувајќи ги правните можности за употреба на беспилотни летала за работа и бизнис.

Во Македонија постои регулатива за тоа како можат да се користат беспилотните летала, а објаснето е во „Службен весник на Р.М. бр. 13 од 28.1.2015". Оваа регулатива ги дефинира сите дозволени операции заедно со процесот за регистрација на беспилотни летала. Оперативната дозвола за тежина на беспилотни летала од 20 до 150 кг ја издава Агенцијата за цивилно воздухопловство, но овие прописи за утврдување на пловидбеноста на беспилотните летала не се во согласност со стандардите на ICAO. Постои дефинирано упатство издадено од Агенцијата за цивилно воздухопловство за сите услови во подготовката, дизајнот и користењето на беспилотни летала. Само пилотите со сертификати од Агенцијата можат да вршат какви било операции со беспилотни летала. За сите операции со беспилотни летала, АТЦ мора да добие порака за планираниот лет пред да се случи.

Досега бизнисите користеле беспилотни летала главно за видео и фотографија, особено за маркетинг-цели, но има многу други примени за UAV-технологијата. Беспилотните летала се повеќенаменски инструменти кои нудат потенцијал за повторно да се одредат некои од најкритичните начини на кои работи човештвото. Некои од индустриите кои почнуваат да користат беспилотни летала се:

- Архитектура и градежништво
- Земјоделство
- Беспилотни летала како услуга
- Беспилотни летала за испорака
- Служби за итни случаи
- Инженерство

- Медиуми
- Следење на животната средина
- Обука
- Видеонадзор

Затоа ни е потребна анализа на ризиците за заштита на приватноста и заштитата на податоците кои произлегуваат од овие уреди и напорите во Европа за да се воспостави рамка за решавање на проблемите. Постојат два аспекта: прво, сегашните правила за заштита на податоците во Европската Унија (ЕУ) кои ги опфаќаат импликациите за граѓанските слободи на потенцијалната употреба на постојани пловни системи за следење, а второ, идејата дека стандардите за приватност имаат улога на поддршка на регулативите бидејќи тие можат да имаат додадена вредност со ублажување на некои ризици за приватноста и промовирање на усогласеноста на операторите на беспилотни летала и на контролорите на податоците со принципите за заштита на податоците.

Цитат од „Влијанијата на приватноста и заштитата на податоци за цивилна употреба на дронови беспилотни летала“ - Европски парламент:

ПРАШАЊА ЗА ПРИВАТНОСТ И ЗАШТИТА НА ПОДАТОЦИ

Беа покренати голем број на прашања во врска со беспилотните летала и уредите и примените што може да ги носат. Беспилотните летала често се опремени со видеокамера и други носивости може да се инсталираат за да се овозможи собирање и обработка на лични податоци, што може да создаде сериозен ризик за правото на приватен и семеен живот, приватност и заштита на податоците. Обезбедување дека почитувањето и спроведувањето на приватноста и заштитата на податоците се споменува како цел во сите документи поврзани со беспилотни летала, од патоказот кон Европска агенција за воздухопловна безбедност (EACA) - Концептот на оперативниот документ. Овие документи исто така потврдуваат дека почитувањето на приватноста и заштитата на податоците е услов за јавно прифаќање на беспилотни летала во општеството. Главните документи за анализа на влијанието на беспилотни летала врз овие основни права се одговорот на Работната група 29 за заштита на податоците на прашалникот 25 на Комисијата, мислењето 26 на Европскиот супервизор за заштита на податоци (ЕДПС) и Студијата на Комисијата за приватност, заштита на податоци и етички ризици во граѓанските RPAS-операции, кои ја формираа основата за размислувањата.

ПОТЕНЦИЈАЛНО ВЛИЈАНИЕ НА БЕСПИЛОТНИ ЛЕТАЛА И НИВНИТЕ ПРИМЕНИ ВРЗ ПРИВАТНОСТА И ЗАШТИТАТА НА ПОДАТОЦИТЕ

За да им дозволат да бидат управувани, беспилотните летала обично се комбинираат со апликации како што се фотоапарати или видеокамери (бидејќи далечинскиот пилот мора да види или да открие што е пред беспилотното летало за да се избегне судир). Тие исто така може да ги снимаат сликите преку софтвер за обработка на видеослики, кои можат да имаат и понатамошни примени (вклучувајќи зумирање со голема моќност, препознавање на лице, профилирање на однесувањето, следење на движење, препознавање на регистарски таблички, термосензори, ноќно гледање, радар, обработка на „види преку слики“ (see-through imaging), сензори за Wi-Fi, микрофони и аудиосистеми за снимање, биометриски сензори за обработка на биометриски податоци, ГПС-системи за обработка на локацијата на снимените лица, системи за читање на IP- адреси и следење на RFID-уреди итн.). Беспилотните летала и нивните примени следствено подразбираат собирање, обработка, евидентирање, организација, складирање, употреба и комбинација на податоци што овозможуваат идентификација на лица, директно или индиректно. Следствено, овие активности подразбираат мешање во правото на приватниот и семејниот живот и заштитата на податоците. Покрај тоа, беспилотните летала претставуваат нови предизвици во однос на приватноста и заштитата на податоците. RPAS-способностите, кога се комбинираат со технологии и апликации, ја менуваат и трансформираат природата на надзорот, зголемувајќи го, во споредба со други слични алатки (сателити, авиони, хеликоптери, систем за видеонадзор): беспилотните летала можат да бидат незабележливи (не се секогаш видливи или слушнати, како што се авиони, хеликоптери, интерни телевизиски камери, особено како што се развиваат мали и микробеспилотни летала). РГ 29 (Работната група 29) работи на нов и посеопфатен документ за беспилотни летала. Беспилотните летала не се слични на птичјиот поглед од сателитите или авионите, или фиксниот поглед на системот за видеонадзор); тие можат да пристапат до повеќе локации (како што се приватни имоти, преку огради или преку прозорци); можат детално да ги набљудуваат (повеќе од голо око, преку зумирање) и лесно да ги следат лицата; тие се евтини (не се скапи како сателитите, авионите или хеликоптерите) и упорни (можат да летаат или да следат некоја личност на одредено време). Сите овие специфичности ги поедноставуваат и подобруваат тајните и отворените надзори и следењето на поединци или групи (вклучително и за време на демонстрации). Студијата на КОМ примени анализа за ризик на приватноста, заштитата на податоците и етиката на серија на RPAS-оператори и мисии кои предложуваат практики за намалување на ризикот. Ризиците што се испитуваат во студијата содржат ризици за приватноста, како што се:

застрашувачкиот ефект од тоа да бидеш гледан, дехуманизација на оние кои се под надзор, транспарентност и видливост, отчетност и воајеризам, злоупотреба на функција, телесна приватност, приватноста на локацијата и просторот, приватноста и асоцијацијата;

ризици за принципите за заштита на податоци, како што се транспарентност, ми-

нимизирање на податоците, пропорционалност, ограничување на намената, согласност, одговорност, безбедност на податоците, права на пристап, права на поправка, трансфери од трети земји, права на бришење; и етички прашања, како што се безбедноста, јавното незадоволство, дискриминација.

Со оглед на високиот степен на потенцијално мешање и упад во правото на приватен живот и заштита на податоците на граѓаните (но и на јавни личности како што се политичари и институционални претставници, личности или претпријатија итн.), важно е дека беспилотните летала и сродните апликации правилно се регулирани за да се обезбеди почитување на основните права, особено на приватноста и на собраните и обработени податоци, низ целиот синџир на беспилотни летала (од производство до акција за спроведување на законот во случај на незаконска употреба), како што треба да се направи за безбедност и сигурност.

ДАЛИ БЕСПИЛОТНИТЕ ЛЕТАЛА ПРЕТСТАВУВААТ ЗАКАНА ЗА ПРИВАТНОСТА?

Вреди да се спомене дека не секоја употреба на дронови задолжително ќе предизвика проблеми со приватноста и заштитата на податоците. Всушност тоа е каде што, на пример, опремата во беспилотното летало овозможува собирање на визуелни слики, звук или геолокација. Оваа опрема може да биде интегрирана во беспилотни летала при купувањето или додадена по пат на растечкиот пазар на продавачите на софтвер и хардвер, кои ги прошируваат можностите и функционалноста на беспилотното летало. Оние што се на земјата, се разбира, не можат да кажат кои вградени функции ги вклучува беспилотното летало кое надлетува над нив, што значи дека перцепцијата за шпионирање може потенцијално да остане без оглед на способностите за собирање на податоци на конкретни беспилотни летала.

Од перспектива за заштита на податоци, собирањето и користењето на лични податоци на поединци (како што се слики, звук или информации за локација) со опрема која е вклучена во беспилотно летало може да биде предмет на Закон за заштита на податоци.

КЛУЧНИТЕ БАРАЊА ЗА ЗАШТИТА НА ПОДАТОЦИТЕ КОИ СЕ РЕЛЕВАНТНИ ЗА УПОТРЕБАТА НА БЕСПИЛОТНИ ЛЕТАЛА ГО ВКЛУЧУВААТ СЛЕДНОВО:

ЗАКОНСКА ОБРАБОТКА - што значи во пракса дека: беспилотните летала што собираат лични податоци мора да се усогласат со сите релевантни закони. Ова ќе биде особено релевантно ако националното законодавство забранува употреба на беспилотни летала, кога е потребно посебно овластување од Надлежниот орган за цивилно воздухопловство (CAA) поради типот или големината на беспилотното летало или начинот на кој се користи или кога националните прописи за Системот за видеонадзор (CCTV) се однесуваат на камери на беспилотни летала; и

една од правните основи во Законот за заштита на податоците, потребна за легитимна обработка, е задоволена. Тука спаѓаат релевантните услови:

согласност - Во пракса добивањето на согласност од субјектите на слики или видеоснимки, на пример, веројатно во многу случаи ќе се покаже за тешко, особено затоа што за да биде валидна, нивната согласност треба да биде слободно дадена, специфична и информирана;

неопходни за договор кога субјектот е странка - ова може да биде релевантно кога беспилотно летало се користи од страна на агент за недвижности според неговиот договор за продажба на имот, да се направи видео само од имотот на сопственикот или алтернативно кога купениот производ е доставен до домот на купувачот од беспилотно летало;

неопходни за правни причини или причини од јавен интерес - како што се одредени ограничени, неопходни и пропорционални употреби на беспилотни летала за спроведување на законот;

строго неопходни за заштита на виталните интереси на субјектот - на пример, употребата на беспилотни летала во одредени случаи од службите за итни случаи за да се лоцираат жртвите на несреќи; или

неопходни за цели на легитимни интереси - ова е предвидено за интересите, правата или слободите на субјектот на податоците да не ги надминуваат оние на контролорот за податоците од беспилотното летало. Тука може да се вклучуваат примери за беспилотни летала што се користат за приватно обезбедување или следење на критичната инфраструктура како што се електрични водови или цевки, како и оние што се користат за следење на животната средина или мапирање на археолошките локации.

ТРАНСПАРЕНТНО И ЈАСНО – што значи дека луѓето треба да бидат свесни за собирањето и обработката на нивните лични податоци. Особено, треба да им се каже кој е контролорот на беспилотното летало, целта на обработката и другите информации, како што се видот на податоци кои се собираат, со кого може да се споделат и нивните права за пристап и поправка на податоците. Јасно е дека употребата на дронови претставува предизвик за тоа како да им дадат јасни и однапред дадени информации на луѓето и поради оваа причина се препорачува да се прифатат голем број на различни пристапи за комуникација на оваа информација, која може да вклучува, на пример:

однапред дадени известувања - на пример, ова може да биде возможно во контекст на спортски или други настани каде информациите може да се обезбедат во литературата пред настанот, програмските материјали и социјалните медиуми. Исто така, може да биде релевантно кога, на пример, агентот за недвижности пишува за однапред да ги информира соседите дека ќе снима евиденција на имот што се продава во нивна близина.

известувања на самото место - вклучувајќи постери и знаци на влезот во дискретни области што се следат со беспилотни летала.

идентификација на беспилотни летала - преземање чекори за да се направи беспилотното летало што е можно повеќе забележливо. Ова може да вклучува, на пример, користење на светли бои, трепкачки светла и звуци на алармирање. Исто така, може да вклучува етикетирање или обезбедување на детали за регистрација на беспилотното летало, што може да биде релевантно ако се изгуби контролата на беспилотното летало и податоците треба да се поврзат со операторот. Употребата на регистарски ознаки исто така може да го обезбеди идниот потенцијал за безжичен пренос на деталите за регистрација на беспилотни летала да се вкрстат со онлајн ресурс кој ги содржи деталите на контролорот на беспилотното летало и неговата употреба.

видливост на операторот - за линија на видување на беспилотните летала операторот може да се направи да изгледа многу видлив и препознатлив како таков.

онлајн ресурси - како што се веб-страници и апликации кои се користат за давање на повеќе информации за тоа зошто, како и каде беспилотните летала имаат и ќе бидат користени од контролорите.

БЕЗБЕДНА ОБРАБОТКА - преземање чекори за обезбедување на лични податоци од каков било неовластен или случаен пристап, откривање, промена или загуба, вклучувајќи далечински сајбер-напади на самото беспилотно летало и каде што личните податоци се пренесуваат од уредот. Ова, на пример, би можело да биде со користење на шифрирање или други соодветни методи за да се заклучи пристап до информациите само до оние ограничени луѓе кои се овластени да ги гледаат или да пристапуваат до снимените слики и податоци.

Не е дозволено да се користат беспилотни летала за следење на вработените без претходна најава и само во случај кога тоа е деловна потреба и во согласност со ГДПР-регулативата. Треба да се развие политика која се однесува на целите за тоа кога и од кого може да се користат беспилотни летала, да биде лесно и трајно достапна за сите вработени, со цел и да ги води за прифатливо и неприфатливо користење на средствата, мрежата и објектите. Ова им овозможува на вработените да го приспособат своето однесување за да спречат да бидат следени кога легитимно ги користат објектите за ИКТ за приватна употреба. Како добра практика, таквата политика треба да се оценува, најмалку еднаш годишно, за да се оцени дали избраното решение за следење ги испорачува предвидените резултати и дали постојат други, помалку инвазивни алатки или средства достапни за постигнување на истите цели.

Затоа, потребата од беспилотни летала и нивната поставеност треба да биде целосно оправдана со цел да се постигне соодветна рамнотежа помеѓу легитимните интереси и основното право за заштита на личните податоци на вработените. За да може да се смета на легитимните интереси на работодавачот, треба да се преземат одредени мерки за ублажување на ризиците.

КАМЕРИ КОИ СЕ НОСАТ (СКРИЕНИ КАМЕРИ)

Видео што се носи на тело (Body Worn Video - BWV), исто така познато како камери за тело и камери кои се носат на тело, или камери што може да се носат е аудио, видео или фотографски систем за снимање кој може да се носи.

Видеото што се носи на тело има голем број на намени и дизајни, од кои две познати употреби се „Гугл очила“ и како дел од опрема за полициска работа. Други употреби вклучуваат акциони камери за социјални и рекреативни намени (вклучувајќи велосипедизам), во рамките на трговијата, во здравството и медицинската употреба, во воена употреба, новинарство, надзор на граѓаните и прикриен надзор.

Скриена камера или шпионска камера или безбедносна камера е статична или видеокамера која се користи за снимање луѓе без нивно знаење. Терминот „скриена камера“ вообичаено се користи во реални ТВ-емисии, понекогаш кога субјектите не се свесни дека се снимаат, а понекогаш со нивно знаење и согласност. Терминот „шпионска камера“ обично се користи кога субјектот вообичаено се очекува да приговара на тоа да биде снимен како упад во нивната приватност. Терминот „безбедносна камера“ најчесто се користи за да се обезбеди оправдување за тајно снимање и може да се контрастира со системот за видеонадзор, што е видливо и кое понекогаш е придружено со предупредување за неговото присуство.

Камерата може да биде „скриена“ затоа што не е видлива за субјектот што се снима, или е преправена како друг предмет. Таква камера можеби нема да биде видлива за

субјектот, на пример, бидејќи е опремена со објектив со долг фокус и се наоѓа надвор од прегледот на субјектот или се наоѓа, на пример, зад двонасочно огледало. Скриени камери може да се вградат во често користени објекти како што се телевизори, детектори за чад, радио со часовник, детектори за движење, капа, растенија и мобилни телефони. Скриени камери може да се користат за набљудување на домаќинствата и исто така, можат да се користат комерцијално или индустриски како безбедносни камери. Производството и намалените трошоци на уредите за видеоснимање доведоа до зголемување на употребата на скриени камери за легитимна потреба за надзор, како и за забава и други цели.

Употребата на скриени камери покренува прашања за лична приватност и може да има правни аспекти кои треба да се земат предвид, во зависност од надлежноста во која се одвива.

Во Македонија сè уште нема соодветно законодавство за камери кои се носат на телото. Постои само Упатство во процес на подготовка, но сè уште не е одобрено.

Камерите за носење често се користат од страна на полицијата во неколку земји за да ги евидентираат нивните интеракции со јавноста или да собираат видеодокази на места со криминал. Се предлага да се зголеми одговорноста на службениците и граѓаните, иако се аргументира дека камерите за носење првенствено ја штитат полицијата. Бидејќи трауматските настани може да имаат влијание врз меморијата, камерите исто така овозможуваат репродукција преку видео во случај на губење на меморијата.

ЗАГРИЖЕНОСТ ЗА ПРИВАТНОСТ

Загриженост во врска со приватноста е покренатa со оваа технологија, на пример, во контекст на Гугл очила (Google Glasses) и полицијата.

Иако оваа опрема има корист во одредени ситуации, постои загриженост во врска со собирање податоци од голем обем, во комбинација со препознавање на лице и други технологии кои се способни за толкување на видеа во најголемиот дел, значи дека секоја употреба на такви камери потенцијално создава средство за следење на голем дел од населението во кое било време или место каде што можат да одат другите луѓе.

При полициско работење, секој полициски службеник кој ја носи оваа технологија може да стане „камера за надгледување“ и со технологијата за препознавање на лице, ова може да стане огромно влијание врз секојдневниот живот на луѓето, особено оние кои се со мала сличност со саканиот бегалец или терорист. Ова може да доведе не само до зголемување на случаите на полициско малтретирање, туку и до случаи на расна пристрасност. Исто така постојат и прашања во врска со законите за согласност на странката. Во контекст на снимањето, најголемите проблеми произлегуваат од тоа дали е потребна согласност од една или сите странки пред да се снима разговор или интеракција.

КАКО ДА СЕ КОРИСТИ СКРИЕНА КАМЕРА НА ТЕЛОТО

Актите за заштита на податоците ги поставуваат одговорностите за организациите или лицата (контролори на податоци) кои ги поседуваат и контролираат употребите на информации и ги обезбедуваат правата на поединците во врска со обработката на нивните информации.

Постојат голем број на разгледувања за заштита на податоците кои треба да се исполнат во врска со користењето на системите за следење, бидејќи генерално тие јасно вклучуваат обработка на лични податоци и мора да се усогласат со барањата за транспарентност на Законот за заштита на податоците.

Општо земено, не постои голема тешкотија од перспективата за заштита на податоците, со употребата на CCTV-камери за безбедносни цели. Употребата на опрема за следење (ограничена на снимање на слики) мора да биде во согласност со барањата за транспарентност на Законот за заштита на податоците. Се очекува дека поединците се свесни за постоењето на надзорот и се јасно информирани за сите цели за кои ќе се користат личните податоци, на пр. безбедносни цели; лицата кои ќе имаат пристап до овие информации и колку долго ќе бидат задржани овие информации. Меѓутоа, употребата на уреди кои се носат на тело или други уреди за снимање на слики, кои по својата природа се мобилни, претставуваат потешкотии од перспектива за заштитата на податоците и на приватноста, бидејќи тие можат да доведат до ненамерни снимки.

ЗАКОНОДАВСТВО ЗА КАМЕРИ КОИ СЕ НОСАТ НА ТЕЛОТО

Камерите што се носат на тело се уреди за снимање кои полициските службеници ги носат како дел од нивните униформи за да го документираат она што го гледаат додека ги извршуваат своите должности. Камерите за тело и понатаму се значаен фокус на законодавецот, бидејќи разгледуваат и донесуваат закони за регулирање на односите меѓу полицијата и заедницата.

Општо земено, целта на програмата за камери за носење на тело е да ги евидентира интеракциите на полициските службеници со јавноста во текот на нивните должности. Камерите за носење на тело обично се користат за собирање докази и заштита на полициските службеници од неосновани обвинувања за несоодветно однесување. Друг значаен аргумент за камерите за носење е подобрување на полициската одговорност и професионализам. Со оглед на овој контекст, како и зголемениот квалитет на снимките и чувствителноста на микрофоните, сликите и звукот фатени од камерите за носење на тело во најголем дел ќе бидат за идентификуваните поединци. Според тоа, снимките ќе се сметаат дека содржат лични податоци и ќе бидат предмет на националните закони за заштита на личните податоци.

Поради сето горенаведено треба да има вистинска рамнотежа помеѓу приватноста и потребите за спроведување на законот.

ЕЛЕКТРОНСКО СЛЕДЕЊЕ (МОНИТОРИНГ) НА ВРАБОТЕНИТЕ

Тековните достигнувања во технологијата и можноста за следење и надгледување на податоците доведоа до друг вид на мониторинг наречен електронско следење на вработените. Работодавците одлучија да ги надгледуваат своите вработени за да ја зголемат својата работна сила, па во последниве години се има зголемено надзорот над вработените. Постојат две страни на оваа приказна, работодавците се обидуваат да ја зголемат својата продуктивност, а од друга страна вработените тоа го гледаат како повреда на нивната приватност. Кој е во право и каде е усогласеноста со законите и прописите за заштита на личните податоци?

Како електронско следење, се смета не само видеонадзор и други надзорни активности, туку исто така и пријавување во сите активности на системот, активности за логирање на деловни системи, пријавување на електронска контрола на пристап на физички безбедна област и пријавување на која било активност и однесување што може да се фати со електронски (дигитални уреди).

Вообичаено, следењето на електронските комуникации на работното место (на пример, телефон, интернет-прелистување, е-пошта, инстант пораки, VOIP итн.) се смета како главна закана за приватноста на вработените. Од друга страна, постои потреба да се земат предвид технолошките случувања кои овозможија понови, потенцијално поупадливи и продорни начини на надгледување. Ваквите настани вклучуваат, меѓу другото:

- Алатки за превенција на загуба на податоци (DLP), кои ги следат појдовните комуникации со цел откривање на потенцијални злоупотреби на податоците;
- Системи за заштитни ѕидови за идните генерации (NGFWs) и системи за управување со унифицирани закани (UTM), кои можат да обезбедат различни технологии за следење како што се длабинска инспекција на податоци, пресретнување на TLS, филтрирање на веб-страници, филтрирање на содржини, известување преку уредот, информации за кориснички идентитет и (како што е опишано погоре) превенција на загуба на податоци. Таквите технологии, исто така, можат да бидат распоредени поединечно, во зависност од работодавачот;
- безбедносни апликации и мерки кои вклучуваат пријавување на пристап на вработениот до системите на работодавачот;
- eDiscovery технологија, која се однесува на секој процес во кој електронските податоци се пребаруваат со цел да се користат како доказ;
- следење на апликацијата и користење на уредот преку невидлив софтвер, било на работната површина или во облакот;
- употребата на канцелариски апликации на работното место што се обезбедува

како облак услуга, која во теорија овозможува многу детално најавување на активностите на вработените;

- постојат одредени случаи кога компаниите дозволуваат употреба на уреди во лична сопственост, кои вообичаено се нарекуваат „донеси свој уред". Следењето на личните уреди (пр. компјутери, мобилни телефони, таблети), кои вработените ги обезбедуваат за нивната работа во согласност со специфична политика за користење, како што се „Донеси свој сопствен уред" (BYOD), како и управување со мобилни уреди (MDM) технологија која овозможува дистрибуција на апликации, податоци и конфигурациски поставки и закрпи за мобилни уреди; и
- употребата на уреди што може да се носат (на пример, уреди за здравје и фитнес).

Можно е работодавачот да спроведе решение за „сè-во-едно" следење, како што е збирот на безбедносни пакети што им овозможува да ја следат целата употреба на ИКТ на работното место, наспроти само е-пошта и/или надгледување на веб-страниците како што порано беше случајот. Заклучоците усвоени во Работниот документ за надзор на електронските комуникации на работното место на Работната група 29 (WP55) ќе се применуваат за секој систем кој ќе го овозможи таквото следење.

Пример: Треба да се развие политика која се однесува на целите за тоа кога и од кого може да се пристапи до сомнителни записи за податоци и да бидат лесно и трајно достапни за сите вработени, со цел исто така да ги води за прифатливо и неприфатливо користење на мрежата и објектите. Ова им овозможува на вработените да го приспособат своето однесување за да спречат да бидат набљудувани кога легитимно ги користат ИТ-работните капацитети за приватна употреба. Како добра практика, таквата политика треба да се проценува, најмалку еднаш годишно, за да се оцени дали избраното решение за следење ги испорачало предвидените резултати и дали постојат други, помалку упадливи алатки или средства достапни за постигнување на истите цели.

СЛЕДЕЊЕ НА Е-ПОШТА НА ВРАБОТЕНИТЕ

Следењето на вработените на работа вклучува обработка на лични податоци и како такво, е регулирано со ГДПР. Законодавството го надгледува Канцеларијата на комесарот за информации („ICO") кој го изработил Кодексот за практики за вработувањето („ICO-кодекс"), обезбедувајќи насоки во оваа област за да им се помогне на работодавачите да ги следат законските барања.

ICO-кодекс

Ico-кодексот нагласува дека приватниот живот на вработениот се протега до

работното место, а вработените очекуваат приватност на работното место дури и кога се информирани дека може да се одвива надгледување на работното место. Ова не ги спречува работодавачите да ги следат вработените на работното место, но треба внимателно да се размисли пред да се изврши какво било следење.

Работодавците треба, како минимум, да ги преземат следните чекори пред да извршат следење:

- Преземи проценка на влијанието врз заштитата на податоците („ПВЗП“).
- Ова не мора да биде формално или комплицирано, туку треба да ја идентификува целта на следењето, негативното влијание врз вработените, дали има помалку упадливи средства за постигнување на целта и дали следењето е оправдано.
- Размислете и документирајте ги правните основи за обработка на лични податоци во контекст на следење.
- Согласноста најверојатно нема да биде валидна во контекст на вработувањето, но легитимните деловни интереси на работодавачот може да бидат важечки во зависност од околностите.
- Информирајте ги вработените дека може да се одвива следењето.
- Политиката треба да ја вклучува природата и степенот на следењето и фактот дека може да се пристапи на содржината на пораките.
- Користете ги информациите добиени преку следење само за целите за кои е извршено следењето.
- Освен ако следењето не води до откривање на активност која работодавачот не може разумно да се очекува да ја игнорира.
- Чувајте ги безбедни сите лични податоци добиени преку следењето и трајно да ги избришете кога повеќе не се потребни.
- Ова вклучува ограничување на персоналот кој има пристап до податоците и обезбедување соодветна обука за заштита на податоци.

Мислење на РГ 29

РГ 29 даде свое мислење за обработката на податоците на работа. Ова мислење ги одразува истите теми како и ICO-кодексот, но обезбедува доследни насоки со оглед на најновите технолошки достигнувања кои овозможуваат поупадливо и продорно следење. Мислењето истакнува дека работодавците мора да ја разгледаат пропорционалноста на следењето и дали може да се преземат други активности за ублажување или намалување на обемот и влијанието на следењето врз приватноста на вработениот. Вработените, исто така, треба да бидат информирани (преку разбирлива и лесно достапна политика за следење на работното место) на кое било следење,

неговите цели и околности и нивото и областите на контрола кои вработените ги имаат над нивните податоци.

Одлука на Европскиот суд

Европскиот суд за човекови права („ЕСЧП“) неодамна донесе одлука во случајот на Бабулеску (Bărbulescu), давајќи насоки за степенот до кој комуникациите на вработените може да се следат на работното место. Овој предмет се однесувал на вработен (Б) кој бил отпуштен поради прекршување на политиката на неговиот работодавач кој навел дека употребата на работните компјутери за лична употреба била забранета. Работодавецот доставил записници од персоналните комуникации на Б за време на дисциплинската постапка за да покаже дека имало прекршување на политиката. ЕСЧП сметал дека работодавачот го прекршил правото на приватност на Б затоа што не го информирал однапред за следењето, ниту, пак, му кажал дека може да пристапат до содржината на неговите комуникации. Претходните судови, исто така, не успеале да ги утврдат причините кои го оправдуваат следењето и дали биле пропорционални со целта или дали работодавачот можел да употреби помалку нападни мерки за да го постигне истиот резултат.

Што значи сè ова во пракса?

- Работодавците можат да ги следат е-пораките на вработените на работа, но треба да ги разгледуваат крајно внимателно и грижливо.
- Следете го ICO-кодексот и мислењето на РГ 29, вклучувајќи го и спроведувањето на ПВЗП пред да направите какво било следење, земајќи предвид дали е можно да се постигне целта преку помалку нападни средства и да се осигураат политики кои јасно ги известуваат вработените за следењето, зошто и дека содржината на пораките може да биде видена.
- Ако е-пораките се идентификуваат или се јасно означени со „лични“ не се отвораат освен ако постои реален ризик од сериозна штета на бизнисот, а кога е можно, однапред информирајте го работникот дека содржината може да биде видена.

Сепак, овие пораки се важен потсетник за работодавците дека постојат неколку фактори кои мора да се разгледаат пред да одлучат да ја следат е-поштата на вработениот, вклучително и:

- да се осигура дека вработениот е предупреден дека е-пораките испратени од работниот компјутер може да се следат. Идеално, ова предупредување треба да се наведе во политиката за ИТ и електронски комуникации или договорот за вработување; и
- утврдување на целта на следењето и дали тоа може да се постигне преку какви било помалку нападни средства.

СЛЕДЕЊЕ НА ВРАБОТЕНИТЕ ПРЕКУ КОРИСТЕЊЕ НА СИСТЕМ ЗА ВИДЕОНАДЗОР (CCTV)

Видеоследењето и надзорот продолжуваат да презентираат слични прашања за приватноста на вработените како и претходно: способноста постојано да го доловува однесувањето на работникот. Најсоодветните промени во врска со примената на оваа технологија во контекстот на вработување се способноста за лесен пристап до собраните податоци од далечина (на пр. преку паметен телефон); намалувањето на големината на камерите (заедно со зголемувањето на нивните можности, на пример, со висока дефиниција); и обработката што може да се изврши со нова видеоаналитика.

Со способностите дадени со видеоаналитиката, можно е работодавачот да ги следи изразите на лицето на работникот со автоматски средства, да ги идентификува отстапувањата од предефинираните шеми на движење (на пример, фабрички контекст) и повеќе. Ова би било непропорционално со правата и слободите на вработените, а со тоа и генерално незаконско.

Обработката, исто така, најверојатно ќе вклучува профилирање, а можеби и автоматизирано донесување одлуки. Затоа, работодавците треба да се воздржат од употреба на технологии за препознавање на лицето. Може да има некои дополнителни исклучоци од ова правило, но таквите сценарија не можат да се користат за да се повика на општо одобрување на користењето на таквата технологија.

СЛЕДЕЊЕ НА ОДНЕСУВАЊЕТО НА ВРАБОТЕНИТЕ НА ИНТЕРНЕТ И ВО РАБОТНИОТ ПРОСТОР

Мнозинството работодавци ги следат своите вработени. Тие се мотивирани од загриженоста поради судски постапки и зголемената улога што електронските докази ги имаат во судските постапки и истрагите на државни институции. Додека вработените може да чувствуваат дека таквото следење е повреда на нивните права за приватност, многу видови на следење се дозволени според законот.

Технологијата им овозможува на работодавачите да следат многу аспекти на активностите на работното место на своите вработени. Работодавците користат технологија за да обезбедат увид во однесувањето на вработените врз основа на патеката на „digital footprints“ што се создаваат секој ден на работното место. Оваа технологија може да ги спои сите овие електронски записи за да обезбеди модели на однесување што работодавачите може да ги искористат за да ги оценат перформансите и однесувањето на вработените. На пример, може да се бараат модели на зборови, промени во јазикот или стилот и модели на комуникација помеѓу поединци. Ова им овозможува на работодавачите да ги следат многуте аспекти на работните места на своите вработени, особено на телефони, компјутерски терминали, преку електронска пошта и говорна пошта и кога вработените се на интернет.

Речиси сè што се прави на канцелариското компјутер може да се следи. Ваквото следење е практично нерегулирано. Затоа, освен ако политиката на компанијата конкретно не наведува поинаку (па дури и тоа не е обезбедено), вашиот работодавач може да ги слуша, да ги гледа и чита повеќето од вашите комуникации на работното место. Судовите често откриле дека кога вработените користат опрема на работодавачот, нивното очекување за приватноста е ограничено.

Важно е да бидете свесни дека ветувањата на вашиот работодавец во однос на прашањата поврзани со приватност на работното место можеби не се секогаш законски обврзувачки. Политиките можат да се доставуваат на различни начини: преку прирачници за вработените, преку меморандуми и во синдикалните договори. На пример, ако работодавачот експлицитно наведува дека вработените ќе бидат известени за телефонското следење, работодавачот генерално мора да ја почитува таа политика. Обично постојат исклучоци за истраги за погрешно однесување. Ако сè уште не сте свесни за политиките на работодавачот за приватност на работното место, добра идеја е да се информирате.

Ако имате компјутерски терминал или работна станица на вашата работа, тоа може да биде прозорец на вашиот работодавач во вашиот работен простор. Постојат неколку видови на компјутерско следење:

- Работодавците можат да користат компјутерски софтвер што им овозможува да видат што е на екранот или што се чува во компјутерските терминали и хард дискови на вработените. Работодавците можат да го следат користењето на интернет, како што се веб-сурфање и електронска пошта.
- Работодавците можат да го следат времето кое еден вработен го поминува надвор од компјутерот или времето на мирување на терминалот.
- Следење на удар на тастатурата му наведува на работодавецот колку удари на тастатурата на час извршува секој вработен. Исто така, може да ги информира вработените ако се над или под стандардниот број на удари на тастатура од тоа што се очекува.

СЛЕДЕЊЕ НА ВРАБОТЕНИТЕ ПРЕКУ КОРИСТЕЊЕ НА ГПС-УСЛУГА

Технологиите кои им овозможуваат на работодавачите да ги следат нивните возила станаа широко прифатени, особено меѓу организациите чии активности вклучуваат транспорт или имаат значителен возен парк.

Секој работодавач кој користи телематика на возилото ќе собира податоци за возилото и за секој вработен што го користи тоа возило. Овие податоци може да вклучуваат не само локација на возилото (а со тоа и на вработениот) собрани од основните ГПС-системи за следење, но, во зависност од технологијата, богатство на

други информации, вклучувајќи го и однесувањето на возачот. Одредени технологии, исто така, можат да овозможат континуирано следење и на возилото и на возачот (на пр. рекордери за податоци за настан). Работодавачот може да биде обврзан да инсталира технологија за следење во возилата за да покаже усогласеност со други законски обврски, на пр. за да се осигури безбедноста на вработените кои управуваат со овие возила. Работодавецот исто така може да има легитимен интерес за да биде во можност да ги лоцира возилата во секое време. Дури и ако работодавачите имаат легитимен интерес да ги постигнат овие цели, прво треба да се оцени дали е потребна обработка за овие цели и дали вистинската имплементација е во согласност со принципите на пропорционалност и изборност. Онаму каде што е дозволено приватно користење на професионално возило, најважната мерка што работодавачот може да ја преземе за да обезбеди усогласеност со овие принципи е понудата на откажување: вработениот во принцип треба да има можност привремено да го исклучи следењето на локацијата во случај кога посебните околности го оправдуваат ова исклучување, како што е посета на лекар. На овој начин, работникот може по своја сопствена иницијатива да заштити одредени податоци за локацијата како приватни. Работодавачот мора да осигура дека собраните податоци не се користат за нелегитимна понатамошна обработка, како што е следење и евалуација на вработените.

Работодавецот, исто така, мора јасно да ги информира вработените дека уредот за следење е инсталиран во возило на компанијата што тие го возат и дека нивните движења се снимаат додека го користат тоа возило (и дека, во зависност од технологијата која е вклучена, нивното однесување при возењето исто така може да се сними). По можност таквите информации треба да бидат прикажани видливо во секој автомобил, во видното поле на возачот.

Можно е вработените да ги користат возилата на компанијата надвор од работното време, на пр. за лична употреба, во зависност од специфичните политики со кои се регулира употребата на тие возила. Со оглед на чувствителноста на податоците за локацијата, малку е веројатно дека постои правна основа за следење на локациите на возилата на вработените надвор од договореното работно време. Меѓутоа, доколку таква потреба постои, треба да се разгледа имплементацијата која ќе биде пропорционална на ризиците. На пример, ова би можело да значи дека, за да се спречи кражба на автомобили, локацијата на возилото не е регистрирана надвор од работното време, освен ако возилото не остави широко дефиниран круг (регион или дури земја). Покрај тоа, локацијата ќе биде прикажана само во краен случај - работодавачот ќе ја активира „видливоста“ на локацијата, пристапувајќи до податоците кои веќе се складирани од системот, само кога возилото ќе го напушти предефинираниот регион.

ПЕРСПЕКТИВА НА РАБОТОДАВАЧИТЕ

Според истражувањето направено од компаниите Dataquest и IDC, „приближно 22,8 милиони вработени во САД (40 проценти од работната сила со интернет-пристап) секој ден трошат еден или повеќе часови на интернет", што е околу 63 милијарди долари годишно. Ова е голема сума пари, па работодавците се обидуваат да се осигураат дека вработените се всушност на задача и го прават она за што им се плаќа. Многу работодавци ги следат и ги чуваат електронските пораки, снимаат записи за текст, снимаат колку брзо и колку се релевантни ударите на тастатурата, ги следат телефонските повици, посетените веб-страници, времето на најава и одјава, па дури и прават слики од екранот на вработените во одредени периоди.

Некои работодавци ги користат сигналите од RFID-картички или мобилни телефони за да ги следат своите вработени за време на ручекот, паузите за кафе или вработените кои работат надвор од границите на канцеларијата како резултат на нивниот опис на работното место.

Работодавците, исто така, сакаат да ги заштитат своите интелектуални податоци. Споделувањето на клучните финансиски информации, најновите истражувања, внатрешните информации, правните документи може да бидат во вредност од милиони долари и работодавците би сакале да ги следат овие активности.

Друга поента на работодавачите е тоа што опремата, машините, софтверот и пристапот до мрежа се обезбедени од страна на работодавачите, така што тие имаат право да ја следат правилната употреба на овие уреди со цел да се заштити компанијата.

Исто така, работодавачите споменуваат заштита на трети страни, како што се потрошувачите, засегнатите страни, добавувачите, дистрибутерите, доверителите итн… Компаниите се одговорни за сите овие споменати страни.

Накратко, работодавците поради тоа мораат да внимаваат на следново:

ПЕРСПЕКТИВА НА РАБОТНИЦИТЕ

Вработените, од друга страна, го сметаат електронското следење како упад во нивната приватност, а особено како длабоко кршење на нивното уставно право. Електронски следените вработени тврдат дека работат под стрес. Тие, исто така, веруваат дека електронскиот надзор сериозно го намалува моралот на вработените и му наштетува на односот на доверба изграден помеѓу работодавците и вработените. Милер (2000) (Сејми Милер и Џон Веккерт - Мониторингот од филозофска гледна точка, страница 256) го опишува ова како:

„Постојат и други важни работи во животот, покрај ефикасноста и профитабилноста. Особено, постои правото на приватност. Постоењето на правото на приватност и

сродните права, како што се доверливоста и автономијата, е доволно за да се поткопаат екстремните ставови како што е ставот дека вработените треба да бидат под надзор секоја минута од денот."

Од друга страна, некои вработени ја сакаат идејата да бидат набљудувани, тие би сакале да се одвојуваат поради работата што ја прават и би сакале да ја видат оваа разлика на платата.

ЕТИЧКИ ПРАШАЊА ЗА ЕЛЕКТРОНСКОТО СЛЕДЕЊЕ:

Секој има различни вредности и верувања, па тешко е да се утврди што е етичко или не. Ние можеме да го истражиме ова прашање од различни перспективи како што се:

ПРИВАТНОСТ:

Електронското следење може да ја одземе приватноста на вработените, но е од клучно значење за една организација некако да ги следи своите вработени. Нивото на надзор е многу важно. Вработените мора да знаат дека се надгледувани. Приватноста и правото на вработените мора да се почитуваат за да имаат доверлив однос во корист на компанијата, вработените и третите лица.

Електронското следење се чини дека е во корист на вработените ако го исклучиме прашањето за приватност.

БЕЗБЕДНОСТ:

Електронското следење може да обезбеди пристап до интелектуалните сопствености на компанијата. Компаниите имаат право да ги заштитат своите извори и правилно да ги следат. Распределбата и споделувањето на овие документи прекршува многу политики на компанијата и треба да биде надгледувано. Во прилог на оваа небрежност од страна на опремата обезбедена од работодавачот е друга етичка точка во корист на работодавачот.

МЕРЕЊЕ НА ПРОДУКТИВНОСТА:

Компаниите се организации базирани на профит и во нивен најдобар интерес треба да биде мерењето на продуктивноста. Но, ова е многу деликатна линија, бидеј-

ќи продуктивноста исто така зависи од моралот и работата на вработените. Продуктивноста мора да се мери, но во исто време моралната средина и довербата мора да се одржува на високо ниво.

За ова можете да најдете повеќе објаснувања во упатствата за технологија и приватност.

Заклучок: Во секој случај, доколку треба да се воспостави и спроведе следење, треба да се спроведе проценка на влијанието на ризикот. И потоа, врз основа на резултатите од проценката може да се преземат одредени активности и да се спроведе систем на следење.

ПРИВАТНОСТ И ПРАШАЊА ОД ОБЛАСТА НА ЗАШТИТАТА НА ЛИЧНИТЕ ПОДАТОЦИ

ПОВРЗАНИ СО УПОТРЕБАТА НА **ДРОНОВИ**, **СКРИЕНИ КАМЕРИ**, ЕЛЕКТРОНСКО **НАБЉУДУВАЊЕ** НА **ВРАБОТЕНИ**

ДИРЕКЦИЈА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ

бул.„Гоце Делчев“ бр. 18,
П. фах 417, 1000 Скопје,
Р. Македонија

Тел./Факс:
++ 389 2 3230 635