Ekonomické, právne a technické aspekty monitorovania a trasovania osôb v zdravotníckych zariadeniach modernými technológiami

(Výskumná správa pre štátnu správu)

Žilinská univerzita v Žiline
Žilina 2023

Autori: prof. Ing. Tomáš Loveček, PhD., Ing. Martin Boroš, PhD., prof. Ing. Zdeněk Dvořák, PhD., doc. Ing. Katarína Kampová, PhD., Ing. Mária Lusková, PhD., Mgr. Marián Magdolen, PhD., Ing. Ladislav Mariš, PhD., Ing. Erika Skýpalová, Žilinská univerzita v Žiline, Fakulta bezpečnostného inžinierstva, Katedra bezpečnostného manažmentu, Žilina, SR

Oponenti:

Ing. Dalibor Fučík, samostatný odborný referent - oblasť bezpečnosti a krízového riadenia, Osoba zodpovedná za ochranu osobných údajov, Úrad Žilinského samosprávneho kraja, Žilina, SR

doc. Ing. Martin Hromada, PhD., Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky, Zlín, ČR

Ing. Karin Nováková, odborný referent - Útvar krízového riadenia a hospodárskej mobilizácie, Nemocnica Alexandra Wintera, n.o., v zriaďovateľskej pôsobnosti Ministerstva zdravotníctva Slovenskej republiky, Piešťany, SR

Podpora: APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach

Obsah

Zoznam skratiek 4

Úvod 5

1. Ekonomické hodnotenie monitorovania a trasovania osôb v zdravotníckych zariadenia 8

2. Právne aspekty monitorovania a trasovania pohybu osôb modernými technológiami 16

2.1 Právne aspekty spracúvania osobných údajov 19

2.1.1 Zákonnosť, spravodlivosť, transparentnosť 20

2.1.2 Obmedzenie účelu 21

2.1.3 Minimalizácia údajov 22

2.1.4 Správnosť 23

2.1.5 Minimalizácia uchovávania 24

2.1.6 Integrita a dôvernosť 24

2.2 Posúdenie vplyvu na ochranu údajov 25

2.3 Test proporcionality 31

2.4 Posúdenie rizika pre práva a slobody dotknutých osôb a návrh opatrení na ich riešenie 32

3. Monitorovanie pohybu osôb a sledovanie kontaktov v zdravotníckych zariadeniach 34

3.1 Využitie mobilných aplikácií na sledovanie kontaktov 34

3.2 Technologické riešenia trasovania pohybu osôb 37

3.3 Lokalizačné systémy v zdravotníctve 40

Záver 43

Použitá literatúra 45

Zoznam skratiek

APVV	Agentúra na podporu vedy a výskumu
BLE	Nízkoenergetická technológia Bluetooth (Bluetooth Low Energy)
CBA	Analýzu nákladov a úžitkov (Cost Benefit Analysis)
CEA	Analýzu efektívnosti nákladov (Cost Effectiveness Analysis)
CMA	Analýzu minimalizácie nákladov (Cost Minimalisation Analysis)
CUA	Analýzu účelnosti nákladov (Cost Utility Analysis)
DPIA	Posúdenie vplyvu na ochranu údajov (Data Protection Impact Assesment)
ECDC	Európske centrum pre prevenciu a kontrolu chorôb (European Centre for Disease Prevention and Control)
EC	Európska komisia (European Commission)
GDPR	Všeobecné nariadenie o ochrane údajov (General Data Protection Regulation)
GPS	Globálny lokalizačný systém (Global Positioning System)
IEC	Medzinárodná elektrotechnická komisia (International Electrotechnical Commission)
IR	Infračervené žiarenie (Infrared Radiation)
ISO	Medzinárodná šrganizácia pre štandardizáciu (International Organization for Standardization)
NFC	Komunikácia na krátke vzdialenosti Near Field Communication)
NLS	Nemocničný lokalizačný systém
NVP	Čistá súčasná hodnota (Net Present Value)
NFC	Krátkodosahové, vysokofrekvenčné, bezdotykové spojenie (Near Field Communication)
RFID	Vysokofrekvenčná identifikácia (Radio Frequency Identification)
UWB	Ultraširoké pásmo (Ultra-wideband)
ÚOOÚ SR	Úrad na ochranu osobných údajov Slovenskej republiky
VLC	Komunikácia viditeľným svetlom (Visible Light Communications)
VSS	Kamerový monitorovací systém (Video Surveillance System)
QR	Rýchla odpoveď (Quick Response)

Úvod

Zdravotníctvo patrí medzi najdôležitejší sektor, ktorého nefunkčnosť spôsobuje závažný dopad na zdravie a život obyvateľov. V Slovenskej republike, podobne ako v iných krajinách vo svete, patrí zdravotníctvo medzi sektory kritickej infraštruktúry a jeho význam a dôležitosť potvrdzuje nedávno prebiehajúca epidémia COVID-19, ktorá zmenila v dramaticky krátkom čase život i spôsob myslenia takmer celého ľudstva. Ukázala skutočnosť, aká dôležitá je pre celú spoločnosť zdravotná starostlivosť a paradoxne poukázala na výdavky súvisiace so zdravotníctvom ako na investíciu do prosperity a konkurencieschopnosti krajiny v globálnom svete a nielen ako na nutný nákladový faktor.

Zásadná úloha zdravotníctva je a vždy zostane poskytovanie zdravotnej starostlivosti obyvateľom, pričom táto povinnosť vymedzuje v Slovenskej republike Zákon č. 576/2004 Z.z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov. Vo vzťahu k zdravotníckym zariadeniam a epidemiologickej situácií z dlhodobého hľadiska je nevyhnutné definovať a vytvoriť také ochranné opatrenia, ktoré by boli dlhodobo udržateľné a nenarúšali existujúci systém svojimi obmedzeniami, a taktiež by zabezpečili kontinuálne zabezpečovanie zdravotnej starostlivosti.

Podľa Zákona č. 578/2004 Z.z., §7 zdravotnícke zariadenie je prevádzkový útvar zriadený na poskytovanie zdravotnej starostlivosti a služieb súvisiacich s poskytovaním zdravotnej starostlivosti. Medzi zdravotnícke zariadenie patrí napríklad ambulancia, poliklinika, nemocnica, liečebňa, laboratória, stacionár, atď. V súčasnosti je 33 zdravotníckych zariadení v zriaďovateľskej pôsobnosti Ministerstva zdravotníctva Slovenskej republiky (Ministerstvo zdravotníctva Slovenskej republiky, 2023). Zároveň zákon č. 416/2001 Z.z. hovorí o prechode niektorých pôsobností z orgánov štátnej správy na obce a na vyššie územné celky. Okrem iných ide aj o oblasti zdravotníctva a civilnej ochrany. Medzi prenesené kompetencie v oblasti zdravotníctva patrí napríklad:

- zriaďovanie ambulancií vrátane staníc lekárskej služby prvej pomoci a ambulancií v zariadeniach sociálnych služieb,
- zriaďovanie špecializovaných zariadení ambulantnej starostlivosti, polikliník, nemocníc I. typu a nemocníc s poliklinikou I. (obec) resp. II typu (samosprávny kraj),
- súčinnosť na preventívnych programoch.

Medzi prenesené kompetencie v oblasti civilnej ochrany patrí vypracúvanie analýzy územia kraja z hľadiska možných mimoriadnych udalostí.

Ako príklad možno uviesť Žilinský samosprávny kraj, ktorý má v zriaďovateľskej pôsobnosti celkovo päť zdravotníckych zariadení (polikliniky alebo nemocnica s poliklinikou) (Úrad Žilinského samosprávneho kraja, 2023). Na Slovensku je v zriaďovateľskej pôsobnosti samosprávnych krajov celkovo 11 zdravotníckych zariadení.

Kontinuálne zabezpečenie zdravotnej starostlivosti je primárne podmienené personálnym zaistením zdravotníckych zariadení. Personál v zdravotníckych zariadeniach je priamo vystavený hrozbe nákazy. Jednou z možností ako ochrániť a minimalizovať dopady šírenia rôznych (infekčných) ochorení medzi osobami (napr. pacienti, personál, návštevy, dodávatelia, atď.) nachádzajúcimi sa v zdravotníckych zariadení, je monitorovanie a trasovanie ich pohybu. Pod monitorovaním a trasovaním pohybu osôb, môžeme chápať pozorovanie a zaznamenávanie trasy, ktorú človek prešiel v určitom čase a v danom priestore.

Vo všeobecnosti je možné klasifikovať monitorovanie na dve základné skupiny z pohľadu monitorovanej osoby, a to pasívne a aktívne monitorovanie. Medzi pasívne typy monitorovania je možne zaradiť, tie ktoré sú založené na kontrole osôb v určitom časovom intervale. Aktívne monitorovanie, resp. aktívny systém monitoringu predstavuje neustálu kontrolu monitorovanej osoby v danom priestore a čase s využitím moderných technológií (Boroš, 2020), (Yap, 2020). V prípade existencie epidémie, resp. pandémie aktívny monitoring predstavuje flexibilný nástroj, ktorý umožňuje, resp. by umožnil zefektívniť trasovanie osôb a prispieť k minimalizácií dopadov pandémie v danom subjekte. Základným cieľom trasovania osôb je urýchlene identifikovať potenciálne nakazeného človeka a izolovať ho do karantény. Význam tohto opatrenia spočíva v ochrane iných, zdravých členov spoločnosti a zmiernení opatrení, ktoré sa prijímajú vo vzťahu k riadeniu pandémie, resp. epidémie. Toto tvrdenie podporujú aj výsledky výskumu Stanford univerzity, kde vedci vyvinuli matematický model na skúmanie potenciálu sledovania kontaktov na zníženie šírenia koronavírusu (Salomon, 2021). Modelovali programy sledovania kontaktov v kontexte uvoľneného fyzického odstupu, pričom menili percento hypotetických symptomatických infekcií zistených v komunite od 10 % do 90 % v porovnaní so scenármi bez sledovania kontaktov. Zistili, že detekcia prípadov v komunite a úspešné oslovenie kontaktov musia pri sledovaní kontaktov prekročiť 50 %, aby sa výrazne znížil prenos. Tiež zistili, že najúčinnejšie programy - programy

s vysokou úrovňou účinnosti testovania, sledovania, izolácie a karantény - by mohli znížiť celkový prenos takmer o polovicu. Táto výhoda by umožnila značné uvoľnenie fyzických dištančných opatrení a obmedzení verejného zdravia a zároveň by pomohla kontrolovať šírenie COVID-19 (Salomon, 2021), (World Health Organization, 2021).

Z hľadiska riešenia COVID-19, ako aj prípravy na ďalšie pandémie, vystupuje do popredia otázka ďalších investícií, resp. hľadania možností efektívneho vysporiadania sa s takýmito negatívnymi situáciami. Nápor pacientov infikovaných vírusom posunul systémy zdravotnej starostlivosti mnohých krajín na pokraj kolapsu. Prioritou zostáva zlepšenie existujúcich systémov zdravotnej starostlivosti, ktoré majú potenciál zvýšiť celkovú efektívnosť zdravotného systému a zabezpečiť lekárom a zdravotníckemu personálu (sanitárom, zdravotníckym asistentom, zubným lekárom, laborantom, technikom, fyzioterapeutom a ostatným zdravotníckym pracovníkom) vhodné pracovné prostredie a technológie podporujúce napĺňanie ich poslania.

V nižšie uvedenej správe sú sumarizované ekonomické, právne a technické aspekty monitorovania a trasovania osôb v zdravotníckych zariadeniach modernými technológiami, ktoré sú relevantné z pohľadu ich implementovania vo verejné správe, ktorá zodpovedá za oblasť zdravotníctva, t.j. Ministerstvo zdravotníctva SR, obce a samosprávne kraje). Uvedené zistenia sú výsledkom publikovaných výskumných aktivít riešiteľského kolektívu projektu APPV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach.

1. Ekonomické hodnotenie monitorovania a trasovania osôb v zdravotníckych zariadenia

Z pohľadu zaistenia kontinuity poskytovania zdravotnej starostlivosti v zdravotníckych organizáciách je vhodné implementovať v rámci organizácie systém trasovania a monitorovania, ktorý by vytvoril základ pre program ochrany zamestnancov ale i pacientov pred nákazou infekčnými ochoreniami (napr. respiračným ochorením COVID-19) a taktiež by vytvoril predpoklady na výrazné zníženie celkového prenosu ochorenia. Investícia do takéhoto opatrenia je strategickým rozhodnutím vedenia organizácie z pohľadu ekonomického hodnotenia, ale aj z pohľadu zaistenia poskytovania zdravotnej starostlivosti (Kampova, 2019).

Ekonomické hodnotenie v zdravotníckych zariadeniach je kritické nie len z pohľadu ekonomických nákladov, ale aj z pohľadu dodržania legislatívnych požiadaviek zákona (Zákon č. 576/2004 Z.z.). Preto pri využívaní ekonomického hodnotenia je nevyhnuté sa sústrediť na oba tieto aspekty a aplikovať metódy ekonomického hodnotenie, ktoré ich v sebe zahŕňajú. Medzi takéto metódy je možné zaradiť (Yanan, 2020), (Jurkovičová, 2015), (Baleľa, 2008):

- analýzu efektívnosti nákladov (CEA: Cost Effectiveness Analysis),
- analýzu účelnosti nákladov (CUA: Cost Utility Analysis),
- analýzu minimalizácie nákladov (CMA: Cost Minimalisation Analysis),
- analýzu nákladov a prínosov (CBA: Cost Benefit Analysis).

Analýza efektívnosti nákladov (CEA) je metóda systémovej analýzy, ktorá sa používa pri jednokriteriálnom rozhodovaní (Baleľa, 2008). Možno ju použiť napr. pri logistických projektoch, vzdelávacích predškolských programoch, na finančných úradoch, v zdravotníckych zariadeniach. Obsahom metódy je porovnávanie alternatívnych možností realizácie aktivity, resp. projektu v peňažnom ohodnotení priamych nákladov na projekt a očakávanej efektívnosti. Základným východiskom je zadefinovanie programového cieľa, t. j. efektívnosť alternatív je posudzovaná rozsahom, v ktorom je zahrnutý aj špecifikovaný cieľ. Náklady sú v prevažnej miere ohodnocované v peňažných jednotkách (Úrad pre verejné obstarávanie, 2020). Vybraná alternatíva bude tá, ktorá dosahuje najvyššiu efektívnosť daných nákladov. Analýza efektívnosti nákladov sa môže použiť aj pri porovnávaní podobných projektov, ktoré ponúkajú tie isté ciele. Nie je však vhodná na porovnanie alternatív,

ktoré ponúkajú niekoľko cieľov. Ak sa hľadá určitá špecifikovaná úroveň efektívnosti, tak vhodná alternatíva bude taká, ktorá produkuje efektívnosť pri čo možno najnižších nákladoch na jednotku výstupu. V tomto prípade je potrebný taký ukazovateľ, ktorý povoľuje výber medzi rôznymi rozhodnutiami. Túto požiadavku však spĺňa už spomínaná analýza nákladov a prínosov.

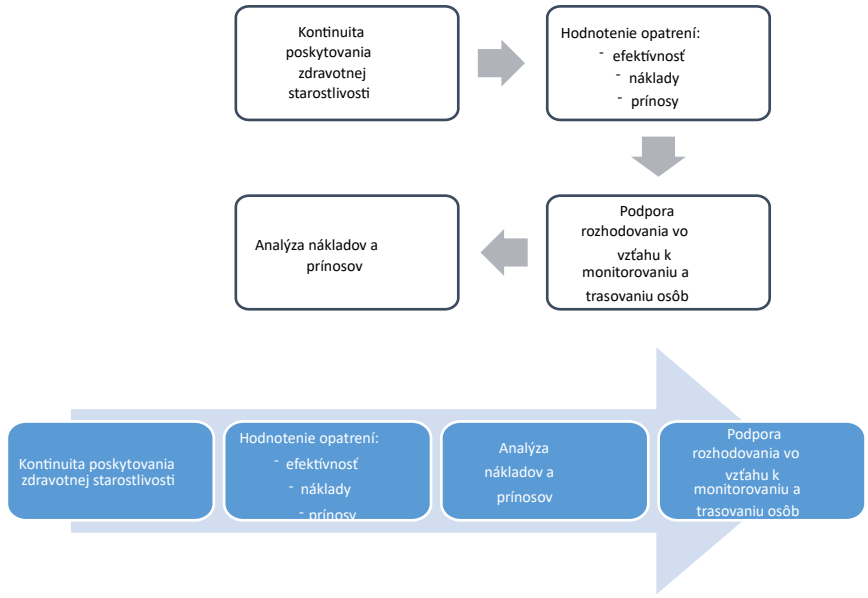
Analýza účelnosti nákladov (CUA) je metodika ekonomickej analýzy, ktorá porovnáva dve alebo viacero alternatív z hľadiska ich nákladov a výsledkov, pričom výsledky sa merajú v jednotkách užitočnosti alebo preferencie - často ako roky zlepšenej kvality života. Je teda variantom analýzy nákladov a prínosov, ktorý vznikol v súvislosti s ekonomickou analýzou zdravia a používa sa predovšetkým pre hodnotenie verejných projektov a programov z oblasti zdravotníctva. CUA sa považuje za zlatý štandard metód pre hodnotenie nákladovej efektívnosti v rámci hodnotenia zdravotníckej starostlivosti (Úrad pre verejné obstarávanie, 2020). K prednostiam CUA v porovnaní s inými metodikami patrí aj skutočnosť, že hodnotí kvalitu poskytovanej intervencie, ktorá je dôležitá v prípade, že dve alternatívy majú rozdielny efekt z hľadiska kvality života a prežitia.

Analýza minimalizácie nákladov (CMA) táto metóda predpokladá, že všetky potenciálne riešenia prinesú rovnaký efekt pri napĺňaní stanoveného cieľa (Beleľa, 2008). CMA patrí medzi najjednoduchšie metódy hodnotenia verejných projektov. Jej predpokladom je zrovnateľnosť a približná zhoda výstupov všetkých uvažovaných alternatív. Najvhodnejšou alternatívou je tá s najnižšími nákladmi. V prípade verejnej zákazky je výberovým kritériom najnižšia cena. Určenie výšky nákladov sa vykonáva pomocou rôznych metód, ako napríklad parametrický odhad nákladov (Úrad pre verejné obstarávanie, 2020), (Sassi, 2001).

Analýza nákladov a prínosov (CBA) je metóda, ktorej cieľom je zvoliť najefektívnejšie alebo najvýnosnejšie voliteľné možnosti na základe porovnávania celkových očakávaných nákladov v peňažnom vyjadrení s ich celkovými očakávanými prínosmi. Analýza môže byť kvalitatívna alebo kvantitatívna alebo môže obsahovať kombináciu kvantitatívnych a kvalitatívnych prvkov a môže sa uplatniť na akejkoľvek úrovni organizácie (Stobierski, 2019). V kvantitatívnej analýze nákladov a výnosov sa peňažná hodnota priradí všetkým hmotným a nehmotným nákladom a prínosom. Často sa stáva, že náklady vzniknú za krátke časové obdobie a prínosy prichádzajú po dlhšom časovom období, preto sa v rámci metódy využíva diskontovanie nákladov a prínosov (Stobierski, 2019), (Lundkvist, 2005).

V rámci analýzy nákladov a prínosov sa z časového hľadiska rozlišujú dva typy analýz. Prvým je analýza ex-ante, ktorá sa využíva v období pred realizáciou projektu, kedy je potrebná pri rozhodovaní o danom projekte alebo pri rozhodovaní o ďalších možnostiach riešenia. Druhým je analýza ex-post, ktorá sa využíva v období po ukončení projektu na zhodnotenie, pričom cieľom je spresnenie dosahov daného projektu v porovnaní s predpokladanými výsledkami pred jeho realizáciou (Kampova, 2019). Z pohľadu obsahu sa analýza nákladov a prínosov skladá z troch hlavných častí: technická časť, finančná analýza aekonomická analýza.

Technická časť je zameraná na definovanie účelu investície - projektu a jeho technickú charakteristiku. Finančná analýza sa zaoberá finančnými nákladmi a výnosmi a jej hlavným cieľom je vyhodnotiť daný projekt z hľadiska finančnej efektívnosti pre investora. Ekonomická analýza súvisí s finančnou analýzou a jej cieľom je hodnotenie prínosov projektu pre všetky subjekty, ktoré sú do neho zapojené (Jurkovičová, 2015), (Sassi, 2001). Grafické znázornenie využitia tejto metódy v rámci rozhodovacieho procese je možné vidieť na obrázku 1.



Obrázok 1 Podpora rozhodovacieho procesu vo vzťahu k monitorovaniu a trasovaniu osôb

V rámci prvého kroku je nevyhnutné sa zamerať na možnosti minimalizácie prerušenia poskytovania zdravotnej starostlivosti, ktorý je základným problémom zdravotníckych zariadení v prípade nekontrolovateľného výpadku zamestnancov v

rámci zdravotníckeho zariadenia. Tieto možnosti minimalizácie sa vzťahujú na identifikáciu možných opatrení, ktoré sú efektívne pri obmedzení šírenia ochorenia. V druhom kroku je potrebné vyhodnotiť účinnosť vybraných opatrení pre jeho zníženie (efektívnosť, výpočet nákladov, výpočet výnosov). V prípade nižšie prezentovaného príkladu bude identifikované opatrenie nástroj na monitorovanie a trasovanie osôb. Tento nástroj je možné využívať v užšom a širšom zmysle. V užšom zmysle sa zameriava iba na zamestnancov zdravotníckych zariadení a znižuje rizika prerušenia poskytovania zdravotnej starostlivosti vo vzťahu k nedostatku kvalifikovaného personálu a v širšom zmysle sa zameriava na monitorovanie a trasovanie všetkých osôb pohybujúcich sa v areáli zdravotníckeho zariadenia.

Hodnotenie efektívnosti monitorovania a trasovania osôb je vyjadrené takou mierou, s ktorou bude riziko odstránené alebo znížené prostredníctvom zavedenia navrhnutých opatrení. Nákladnosť opatrení závisí od porovnania výdavkov a očakávaných prínosov, pričom je potrebné posúdiť efektívnosť vynaložených prostriedkov na uskutočnenie týchto opatrení. Náklady na zavedenie opatrení by mali byť vyčíslené čo najpresnejšie. V poslednom kroku je potrebné aplikovať postupy analýzu nákladov a prínosov tak, aby poskytovali relevantný podklad pre proces rozhodovania. Z výsledkov z analýzy nákladov a prínosov je teda možné získať znalosť o tom, aké efektívne by bolo riešenie daného problému a rozhodneme sa, či tento projekt zrealizujeme alebo nie (Jurkovičová, 2015), (Baleľa, 2008).

Z uvedených metód je CBA vhodným nástrojom podporujúcim proces rozhodovania o implementácií ochranných opatrení. Na základe jej výsledkov je možné prijať optimálne rozhodnutie, nie len z pohľadu nákladov ale i z pohľadu očakávaných prínosov. Prínosy sú v takomto type organizácie výrazným indikátorom efektívnosti použitých zdrojov. Modelový príklad CBA zameraný na implementáciu systému monitorovania a trasovania osôb v rámci vybraného zdravotníckeho zariadenia je popísaný nižšie.

Predmetom záujmu je zdravotnícke zariadenie, ktoré poskytuje služby v oblasti diagnostiky a zdravotnej starostlivosti. V rámci zdravotníckeho zariadenia je zamestnaných 30 špecializovaných doktorov, 50 zdravotných sestier a 25 iného obslužného personálu. Predmetom investície v rámci projektu je nástroj monitorovania a trasovania osôb, ktorého cieľom je minimalizácia šírenia infekčnej choroby medzi týmto personálom.

Prvým krokom je vytvorenie nulového variantu, ktorý predstavuje súčasný stav. Spoločnosť nemá implementovaný aktívny nástroj na monitorovanie a trasovanie osôb. Zamestnanci spoločnosti dodržujú všeobecne prijaté usmernenia a odporúčania Úradom verejného zdravotníctva Slovenskej republiky. V priebehu sledovaného intervalu jedného roka bolo pozitívne identifikovaných 50 osôb, z čoho bolo 25 doktorov, 15 zdravotných sestier a 10 ostatného personálu. Priebeh ochorenia personálu neviedol k žiadnemu úmrtiu a u zamestnancov sa nevyskytli trvalé následky po prekonaní. Celkové náklady zamestnávateľa, ktoré súviseli s práceneschopnosťou zamestnancov, ich zastupovaním a zvýšením počtu služieb a nadčasov bolo vypočítaných na 107 250 Eur.

Okrem už popísaných finančných dopadov boli následkom danej situácie definované aj nepriame finančné dopady vo forme obmedzenia poskytovania zdravotnej starostlivosti, ktorá súvisela s nedostatkom špecializovaných zamestnancov anestéziológie a resuscitácie, týmto výpadkom boli straty definované v hodnote 55 000 Eur, ktoré by zdravotnícke zariadenie získalo, ak by úkony boli realizované. Ostatné vzniknuté náklady súvisiace s odkladom, resp. presmerovaním operácií na iné zdravotnícke zariadenia a nesúviseli s výpadkom anestéziológa, ale s výpadkom špecialistu v potrebnom odbore, v sledovanom období boli ohodnotené v hodnote 30 000 Eur (Tabuľka 1).

Tabuľka 1 Odhadované finančné dopady

Dopad	Typ dopadu	Suma [€]
Priame dopady	Náklady súvisiace s práceneschopnosťou	107 250
Nepriame dopady	Nemožnosť vykonávať plánované operácie	55 000
	Presmerovanie operácií	30 000
Suma celkom		192 250

Predmetom investície v rámci projektu zameraného na monitorovanie a trasovanie osôb je zníženie šírenia infekčného ochorenia (napr. COVID-19) medzi zamestnancami zdravotníckeho zariadenia (a následne pacientmi), a tým zaistenia kontinuálneho poskytovania zdravotnej starostlivosti bez obmedzujúcich faktorov. Systém monitorovania a trasovania bude realizovaný zákazkovým systémom reflektujúci špecifické potreby tohto zariadenia a jeho zamestnancov. Systém môže

byť založený napríklad na technológií RFID, resp. Bluetooth a celkové odhadované investičné náklady pre zdravotnícke zariadenie sú 25 000 Eur a náklady s vývojom a implementáciou systému monitorovania a trasovania do prostredia organizácie sú odhadované na 15 000 Eur.

Okrem spomínaných nákladov je nevyhnutné uvažovať i o personálnom zaistení, ktoré bude vykonávať obslužné činnosti a vyhodnocovať údaje získané týmto systémom. Celkové ročné odhadované náklady na personál, ktorí bude spravovať a riadiť danú technológiu je 20 000 Eur a náklady na údržbu sú vyhodnotené priemerne na každý rok 500 Eur (Tabuľka 2).

Tabuľka 2 Odhad finančných nákladov systému monitorovania a trasovania osôb

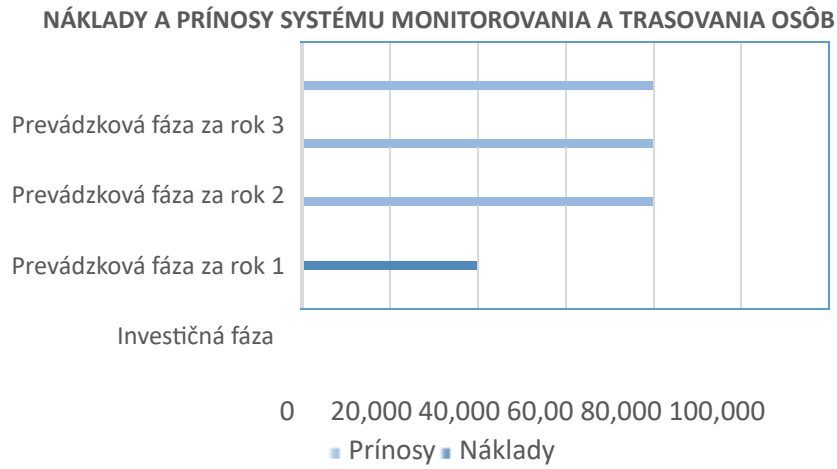
Náklady súvisiace s investíciou	**Popis**	**Suma [€]**
Technológie	Technológií RFID a súčasti systému	25 000
Vývoj a implementácia	Zákazkový projekt	15 000
Personálne obsadenie	Náklady na obslužní a riadiaci personál a technológie / rok	20 000
Údržba	Opravy, straty / rok	500

Ďalšou časťou návrhu systému monitorovania a trasovania osôb je porovnanie finančných dopadov pred a po zavedení tohto systému. V nasledujúcej tabuľke je uvedený možný finančný dopad po zavedení tohto systému do zdravotníckeho zariadenia, ktoré sa opiera o štúdiu Stanford univerzity (Salomon, 2021), ktorá zistila, že najúčinnejšie programy - programy s vysokou úrovňou účinnosti testovania, sledovania, izolácie a karantény - by mohli znížiť celkový prenos takmer o polovicu. Vzhľadom k tomu budeme predpokladať, že implementáciou celkového systému monitorovania a trasovania osôb do zdravotníckeho zariadenia dôjde k zníženiu šírenia medzi zamestnancami o 50%. Tieto výsledky sú prezentované v tabuľke 3.

Tabuľka 3 Odhad možných finančných dopadov po zavedení systému monitorovania a trasovania osôb

Dopad	**Typ dopadu**	**Suma [€]**
Priame dopady	Náklady súvisiace s práceneschopnosťou	53 625
Nepriame dopady	Nemožnosť vykonávať plánované operácie	27 500
	Presmerovanie operácií	15 000
Suma celkom		96 125

Prezentácia nákladov a prínosov systému monitorovania a trasovania osôb je prezentovaná na obrázku (Obrázok 2) za sledované obdobie 4 rokov. Samozrejme v reálnom prostrední by sledované obdobie boli dlhšie.



Obrázok 2 Grafické znázornenie nákladov a prínosov systému monitorovania a trasovania osôb

Na základe kvantifikácie nákladov a prínosov navrhnutého projektu monitorovania a trasovania osôb je možné vypočítať čistú súčasnú hodnotu (NPV) projektu pre každý rok.

$NVP = \sum^{n}_{t=0}(_____1^{CF}{}_{+r}{}^{t})t$, (1)

kde :

NVP - čistá súčasná hodnota investície,

CFt - hotovostný tok plynúci z investícií v období t, r

- diskontná sadza.

Aby bol projekt efektívny musí byť výsledná čistá súčasná hodnota (NPV) kladná, prípadne rovná nule. Kladné hodnoty budú v tomto prípade predstavovať finančné prínosy získané prostredníctvom projektu. V prípade, že by konečná hodnota bola nulová, bude to znamenať, že projekt je prijateľný ale neprináša žiadne finančné prínosy. V tabuľke 4 sú zachytené jednotlivé náklady a prínosy za dané sledované obdobie, ktoré tvoria vstup pre výpočet čistej súčasnej hodnoty.

Tabuľka 4 Kvantifikácia nákladov a prínosov v investičnej a prevádzkovej fáze projektu

Suma [€]	**Investičná fáza**	**Prevádzková fáza (1 rok)**	**Prevádzková fáza (2 rok)**	**Prevádzková fáza (3 rok)**
Náklady	4 0000	25 000	25 000	25 000
Prínosy	0	96 125	96 125	96 125

Konečný výsledok výpočtu čistej súčasnej hodnoty (1) sa porovnáva s kritériami prijateľnosti – čistá súčasná hodnota NPV ≥ 0. Čistá súčasná hodnota (NPV) v prípade tohto projektu vyšla v sume 150 765 Eur za sledované 4 ročné obdobie pri diskontnej sadzbe 5% (Ministerstvo zdravotníctva Slovenskej republiky, 2021). Štvorročné obdobie bolo stanovené ako modelové obdobie. Dĺžka skúmaného obdobia sa definuje na základe požiadaviek konkrétnej organizácie, pretože hovorí o návratnosti investovaných finančných prostriedkov a stanovuje kritérium pre porovnávanie medzi rôznymi projektami. Z uvedeného vyplýva, že implementácia systému určeného na monitorovanie a trasovanie osôb v zdravotníckych zariadeniach, by mala zo strednodobého hľadiska ekonomický prínos. Doba návratnosti tohto systémy by bolo možné ešte skrátiť, pokiaľ by daný systém bol využívaný aj na iné účely (napr. dochádzkový systém zamestnancov, systém kontroly vstupov do vyhradených priestorov, monitorovanie a trasovanie zdravotníckeho materiálu, vyhodnocovanie efektívnosti nastavených procesov – kritické body, prestoje, atď.).

2. Právne aspekty monitorovania a trasovania pohybu osôb modernými technológiami

Pri využití technologických nástrojov, ktoré pre svoje fungovanie budú okrem všeobecných údajov využívať napríklad aj údaje, ktoré svojou povahou zasahujú do súkromia fyzických osôb alebo údaje, pomocou ktorých je možné fyzické osoby identifikovať priamo alebo nepriamo musí byť takéto spracúvanie posudzované s ohľadom na pravidlá spracúvania osobných údajov. Právny rámec pre pravidlá ochrany osobných údajov vytvára v Európskej únii najmä nové Nariadenie Európskeho parlamentu a rady 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (ďalej len „všeobecné nariadenie o ochrane údajov“ alebo „GDPR“). Členské štáty môžu v určitých špecifických situáciách pravidlá GDPR ďalej konkretizovať a upravovať podľa národných požiadaviek. Vhodným zdrojom ako byť v kontakte s aktuálnym ponímaním ochrany osobných údajov je aj sledovanie metodických usmernení národných dozorových orgánov alebo Európskeho výboru pre ochranu údajov.

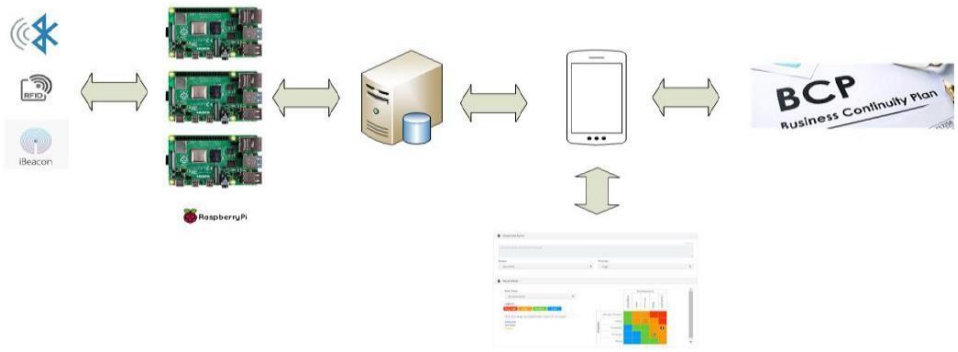
Podľa (GDPR, článok 4) osobné údaje sú akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor, alebo odkazom na jeden či viaceré prvky, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.

Lokalizačné údaje sú všetky údaje spracúvané v elektronickej komunikačnej sieti alebo prostredníctvom elektronickej komunikačnej služby, ktoré udávajú geografickú polohu koncového zariadenia používateľa verejne dostupnej elektronickej komunikačnej služby, ako aj údaje z iných potenciálnych zdrojov týkajúce sa (Usmernenie 4/2020, Príloha):

- zemepisnej šírky, zemepisnej dĺžky alebo nadmorskej výšky koncového zariadenia,
- smeru pohybu používateľa alebo,
- času zaznamenania informácií o polohe.

Spracúvanie osobných údajov je operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov, napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovanie iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami (GDPR, Článok 4, ods. 2).

V prípade monitorovania a trasovania osôb v stavebne ohraničenom priestore (napr. stavebný objekt zdravotníckeho zariadenia) modernými technológiami (napr. RFID, Bluetooth, resp. iBeacon), je možné hovoriť o spracúvaní osobných údajov v rámci počítačových sietí. Z pohľadu spracúvania osobných údajov s využitím moderných technológií je potrebné vnímať v kontexte pojmy ako informačný systém, spracovateľská činnosť a spracovateľská operácia. Podľa (GDPR, článok 4, ods. 6) pojem informačný systém je definovaný ako akýkoľvek usporiadaný súbor osobných údajov, ktoré sú prístupné podľa určených kritérií, bez ohľadu na to, či ide o systém centralizovaný, decentralizovaný alebo distribuovaný na funkčnom alebo geografickom základe. Príklad informačného systému určeného na monitorovanie, trasovanie osôb je uvedený na obrázku (Obrázok 3). Informačný systém v sebe teda môže združovať viacero spracovateľských činností, resp. spracovateľských operácií. Tieto novozavedené pojmy v Nariadení GDPR bohužiaľ nemajú svoju definíciu, ktorá by jasne stanovila ich vzájomnú väzbu na informačný systém. V Nariadení GDPR je iba uvedená definícia pojmu spracúvanie, ako operácia alebo súbor operácií s osobnými údajmi. Tu by bolo možno potrebné doplniť, že spracovateľská operácia je napríklad prenos, záznam alebo zobrazenie a súbor týchto operácií vytvára určitú spracovateľskú činnosť (napr. monitorovanie osôb). Potom informačný systém by bol funkčný celok, ktorý prostredníctvom technických prostriedkov, programových prostriedkov a ľudských zdrojov zabezpečoval túto spracovateľskú činnosť.



Obrázok 3 Bloková schéma informačného systému Cov-ID určeného na monitorovanie, trasovanie osôb a vyhodnotenia rizikovosti možného kontaktu

Podľa (GDPR, Článok 30) každý prevádzkovateľ vedie záznamy o spracovateľských činnostiach, za ktoré je zodpovedný. Vychádzajúc zo vzoru záznamov spracovateľských činností, ktoré zverejnil Úrad na ochranu osobných údajov SR (ÚOOÚ SR) na svojich webových stránkach ako aj z praxe sú príklady spracovateľských činností súvisiacich s monitorovacími systémami uvedené v tabuľke 5.

Tabuľka 5 Príklady spracovateľských činností prevádzkovateľa s využitím monitorovacích systémov

Účel spracúvania	Právny základ	Dotknuté osoby
Monitorovanie a kontrola zamestnancov prostredníctvom kamerového systému	čl. 6 ods. 1 f) Nariadenia GDPR Oprávnený záujem prevádzkovateľa (kontrolný mechanizmus na základe §13 ods. 4 Zákonníka práce)	- zamestnanci prevádzkovateľa - iné osoby, ktoré sa ocitnú (oprávnene alebo neoprávnene) v monitorovanom priestore
Monitorovanie verejných priestorov prostredníctvom kamerového systému za účelom ochrany zdravia a života, bezpečnosti a prevencie kriminality	čl. 6 ods. 1 f) Nariadenia GDPR Oprávnený záujem prevádzkovateľa	- osoby, ktoré sa ocitnú (oprávnene alebo neoprávnene) v monitorovanom priestore

Monitorovanie vozidiel prevádzkovateľa prostredníctvom GPS	čl. 6 ods. 1 f) Nariadenia GDPR Oprávnený záujem prevádzkovateľa	- zamestnanci prevádzkovateľa
Riadenie (monitorovanie) vstupov do vyhradených priestorov (napr.: priestory s vybranými chemickými látkami, liečivami, radiačnými zariadeniami pod.)	čl. 6 ods. 1 f) Nariadenia GDPR Oprávnený záujem prevádzkovateľa	- zamestnanci prevádzkovateľa - zdravotnícky personál
Riadenie, kontrola a logovanie prístupov k elektronickej zdravotníckej dokumentácií	čl. 6 ods. 1 c) Nariadenia GDPR Osobitný zákon č.153/2013 Z.z. o národnom zdravotníckom informačnom systéme a o zmene a doplnení niektorých zákonov	- zamestnanci prevádzkovateľa - zdravotnícky personál
Monitorovanie a trasovanie zamestnancov za účelom ochrany zdravia a života	čl. 6 ods. 1 e) Nariadenia GDPR Plnenie úloh realizovaných vo verejnom záujme (ochrana verejného zdravia)	- zamestnanci prevádzkovateľa
Monitorovanie a trasovanie hospitalizovaných pacientov za účelom ochrany zdravia a života	čl. 6 ods. 1 e) Nariadenia GDPR Plnenie úloh realizovaných vo verejnom záujme (ochrana verejného zdravia)	- pacienti zdravotníckeho zariadenia
Monitorovanie a trasovanie pacientov ambulantnej starostlivosti	čl. 6 ods. 1 a) Nariadenia GDPR Súhlas dotknutej osoby	- pacienti ambulancie

2.1 Právne aspekty spracúvania osobných údajov

Pri akomkoľvek spracúvaní osobných údajov je prevádzkovateľ povinný postupovať v súlade s povinnosťami definovanými vo všeobecnom nariadení o ochrane údajov. GDPR stanovuje šesť základných zásad, od ktorých je možné odvodiť väčšinu povinných krokov pre posúdenie legálnosti spracúvania. Tieto základné zásady vytvárajú logickú a komplexnú sieť otázok, ktoré musí každý prevádzkovateľ pred

spracúvaním osobných údajov zodpovedať a súčasne nastavením budúceho spracúvania v súlade s týmito zásadami zosúladiť právne požiadavky s reálnou aplikáciou v praxi. Na základe (GDPR, Článok 5) základnými zásadami sú:

- zákonnosť, spravodlivosť a transparentnosť,
- obmedzenie účelu,
- minimalizácia údajov,
- správnosť,
- minimalizácia uchovávania,
- integrita a dôvernosť.

V nasledujúcich podkapitolách je rozanalyzované, aké otázky je si pri jednotlivých zásadách potrebné zodpovedať.

2.1.1 Zákonnosť, spravodlivosť, transparentnosť

Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé. Spracúvanie osobných údajov je zákonné v prípade, ak je založené na správnom právnom základe, pričom sleduje legitímny účel spracúvania (Hudecová, 2018). Zákonnosť akéhokoľvek monitorovania, ktoré je vždy výrazným zásahom do súkromia jednotlivca, môže byť s ohľadom na účel spracúvania a typ prevádzkovateľa vykonaný len na základe jedného z určených právnych základov, stanovených v Článku 6 Nariadenia GDPR. Z posúdenia špecifického prepojenia právneho základu, prevádzkovateľa a účelu vyplynie kombinácia, ktorá je nevyhnutná pre dané spracúvanie. Príkladom vhodnej kombinácie je napríklad spracúvanie osobných údajov orgánom verejnej správy na právnom základe plnenia úloh vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi (GDPR, Článok 6, ods. 1, písm. e), pričom účelom by mala byť konkrétna povinnosť takéhoto orgánu stanovená v osobitnom právnom predpise. Menej vhodným príkladom by mohlo byť napríklad monitorovanie zamestnancov na základe súhlasu, kedy by neboli dostatočné záruky a možnosť preukázania, že súhlas zamestnancov bol udelený bez nátlaku a so slobodou voľby odmietnuť dané spracúvanie (najmä s ohľadom na hierarchickú pozíciu medzi zamestnávateľom a zamestnancom).

Z pohľadu spravodlivosti je potrebné zabezpečiť spracúvanie tak, aby dotknutá osoba bola transparentne informovaná o spracúvaní osobných údajov, pričom osobitne by sa mali uviesť podmienky spracúvania najmä s ohľadom na prípadné profilovanie, obmedzenie automatizovaného spracúvania osobných údajov či možnosti uplatnenia všetkých práv dotknutej osoby.

Transparentnosť spracúvania osobných údajov spočíva v otvorenej komunikácii s dotknutými osobami, prípadne aj s dozorovým orgánom. Minimálne informácie, ktoré musí získať dotknutá osoba pred spracúvaním osobných údajov stanovuje GDPR, ale prevádzkovateľ v záujme transparentnosti môže ísť aj nad rámec povinných údajov a zverejniť aj iné podklady pre preukázanie jeho legitímnych záujmov ako nástroja ochrany a dôvery v ochranu súkromia, ktoré dodržiava. Všetky informácie, ktoré smerujú k dotknutým osobám, by mali byť v ľahko dostupnej forme, formulované zrozumiteľne, jasne a jednoducho. Medzi takýmito podkladmi by mohli byť napríklad testy proporcionality, posúdenie vplyvov na ochranu osobných údajov, analýza rizík, jasne definované role zainteresovaných osôb v rozsahu ich práv a povinností, spôsob a možnosť preskúmania spracúvania, odkazy na aktuálny stav poznania najmä s ohľadom na aplikované bezpečnostné a anonymizačné opatrenia a podobne. Európsky výbor na ochranu osobných údajov napríklad pri využívaní aplikácii špecificky uvádza, že: „s cieľom zabezpečiť spravodlivosť a zodpovednosť algoritmov a všeobecnejšie ich súlad s právom, algoritmy musia byť kontrolovateľné a mali by byť pravidelne skúmané nezávislými odborníkmi. S cieľom čo najširšej kontroly by sa mal zverejniť zdrojový kód aplikácie“ (Hudecová, 2018).

2.1.2 Obmedzenie účelu

Definícia účelu spracúvania je kľúčová tak pre posúdenie zákonnosti ale aj pre komunikáciu s dotknutými osobami. Pre naplnenie povinnosti určiť účel spracúvania musí prevádzkovateľ špecifikovať konkrétny, jednoznačný dôvod spracúvania. Tento účel definuje prevádzkovateľ alebo vyplýva z osobitných právnych predpisov, pokiaľ je právnym základom spracúvanie na základe osobitného zákona alebo pri výkone verejnej moci. Z konkrétneho účelu, ktorý je jasný a zrozumiteľný by mali okrem záujmu a zámeru prevádzkovateľa vyplývať aj prínosy pre dotknutú osobu.

Obmedzenie účelu stanovuje zákaz využitia získaných osobných údajov na iné účely než ten, na ktorý boli získané. Hudecová píše, že „zásada obmedzenia účelu predstavuje jednu z kľúčových zásad spracúvania osobných údajov. Je úzko spojená so zásadou zákonnosti, spravodlivosti a transparentnosti, keďže poskytuje dotknutým osobám právnu istotu, že ich osobné údaje môžu byť spracúvané iba na konkrétne určený, výslovne uvedený a legitímny účel. Zároveň predstavuje nevyhnutný predpoklad, pre aplikáciu zásady minimalizácie údajov a minimalizácie uchovávania, a to z dôvodu, že stanovený účel spracúvania osobných údajov

ovplyvňuje rozsah spracúvaných osobných údajov nevyhnutných na dosiahnutie účelu spracúvania, ako aj dobu ich uchovávania“ (Hudecová, 2018).

Hoci Nariadenie GDPR v určitých prípadoch umožňuje zlúčenie účelov, resp. využitie osobných údajov na iný účel ako boli získané, ale k tomu by mal každý prevádzkovateľ pristupovať nanajvýš opatrne. „S cieľom zistiť, či je účel ďalšieho spracúvania v súlade s účelom, na ktorý boli osobné údaje pôvodne získané, by mal prevádzkovateľ po splnení všetkých požiadaviek zákonnosti pôvodného spracúvania zohľadniť okrem iného akékoľvek prepojenie medzi týmito účelmi a účelmi zamýšľaného ďalšieho spracúvania; kontext, v ktorom sa osobné údaje získali, najmä primerané očakávania dotknutých osôb vyplývajúce z ich vzťahu k prevádzkovateľovi, pokiaľ ide o ich ďalšie použitie; povahu osobných údajov; následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby; a existenciu primeraných záruk v pôvodných aj zamýšľaných operáciách ďalšieho spracúvania“ (GDPR, Recitál 50).

2.1.3 Minimalizácia údajov

Minimalizácia údajov predstavuje povinnosť prevádzkovateľa získavať a spracúvať iba také osobné údaje, ktoré sú „primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú“. (GDPR, Článok 5, ods. 1 písm. c). Prevádzkovateľ by mal vždy vykonať dôkladnú analýzu, ktoré osobné údaje potrebuje získavať a tieto obmedziť na striktné minimum. Najmä pri získavaní lokalizačných údajov prostredníctvom moderných technológií je nevyhnutné zisťovať, či sa týmto nezískavajú aj „nesúvisiace alebo nepotrebné informácie, napríklad občiansky stav, identifikátory komunikácie, položky v adresári zariadenia, správy, záznamy hovorov, lokalizačné údaje, identifikátory zariadenia atď“ (Usmernenie 4/2020, bod 40). V prípade trasovania pohybu v zdravotníckych zariadeniach vzniká aj riziko, že určením polohy osoby bude nepriamo zisťovaný aj jej zdravotný stav alebo aspoň jeho indikácie (napríklad prostredníctvom ambulancií, ktoré navštívil, ako dlho sa tam zdržal a pod.). Pri aplikácií zásady minimalizácie údajov je vhodné použiť nástroje pre posúdenie primeranosti a proporcionality.

S ohľadom na minimalizáciu ale aj bezpečnosť osobných údajov je potrebné aby prevádzkovateľ využil nástroje špecificky navrhnutej a štandardnej ochrany osobných údajov. Európsky výbor na ochranu osobných údajov „zdôrazňuje, že pokiaľ ide o používanie lokalizačných údajov, malo by sa vždy uprednostniť

spracúvanie anonymizovaných údajov, a nie osobných údajov“ (Usmernenie 4/2020, bod 14). Avšak pri anonymizácii treba byť opatrný, pretože najmä pri veľkých a podrobných súboroch údajov, kde sú údaje prepojené, je anonymizácia veľmi obtiažna. „V mnohých výskumoch sa skutočne potvrdilo, že lokalizačné údaje, ktoré sa považujú za anonymizované, také v skutočnosti nemusia byť. Stopy mobility jednotlivcov sú vo svojej podstate úzko prepojené a jedinečné. Za určitých okolností preto môžu ľahko podliehať pokusom o opätovnú identifikáciu“ (De Montjoye, 2013) (Pyrgelis, 2017).

Minimalizácia údajov by mala zohľadňovať aj prípadnú vzájomnú komunikáciu s dotknutými osobami a pokiaľ z účelu spracúvania vyplýva aj spätné odovzdávanie informácií (napríklad vo forme informovania osôb o blízkom kontakte s osobou nakazenou ochorením Covid 19 a pod.) je potrebné aj odosielané informácie podrobiť testu primeranosti, aby z nich napríklad neoprávnene nevyplynuli závery zasahujúce do súkromia inej osoby než tej, ktorá je informovaná (napríklad o identite nakazeného).

2.1.4 Správnosť

Zásada správnosti predpokladá využitie iba správnych a podľa potreby aktualizovaných osobných údajov. Prevádzkovateľ je povinný prijať všetky potrebné opatrenia, aby sa zabezpečilo, že sa osobné údaje, ktoré sú nesprávne z hľadiska účelov, na ktoré sa spracúvajú, bezodkladne vymažú alebo opravia.

Hoci GDPR nestanovuje čo je nesprávny údaj, prevádzkovateľ by mal „nastaviť interné postupy na overovanie správnosti získavaných, ako aj následne spracúvaných osobných údajov a podľa potreby aj postupy na zabezpečenie ich aktualizácie. Zložitosť uvedených interných procesov bude závisieť od viacerých okolností, najmä od povahy spracúvaných osobných údajov a účelu ich spracúvania, ako aj od skutočnosti, do akej miery môže spracúvanie ovplyvniť dotknutú osobu“ (Hudecová, 2018). Zavedené interné postupy môžu byť zverejnené s ohľadom na zásadu transparentnosti.

Spoločne s overovaním správnosti údajov by mal byť nastavený aj proces možnosti/povinnosti opraviť údaje, najmä ak ich spracúvanie môže mať veľký vplyv na jednotlivcov. Toto by sa, samozrejme, malo vzťahovať iba na prípady, keď sa údaje spracúvajú spôsobom, ktorý takúto opravu technicky umožňuje, a v prípadoch, keď sa pravdepodobne vyskytnú uvedené nepriaznivé účinky (napríklad pri použití

lokalizačných údajov v prípade ak zle zaznamenaná poloha bude mať vplyv na poskytnutie služby alebo priamy dôsledok pre dotknutú osobu).

2.1.5 Minimalizácia uchovávania

Zásada minimalizácie uchovávania vyjadruje povinnosť prevádzkovateľa uchovávať osobné údaje vo forme, ktorá umožňuje identifikáciu dotknutých osôb najviac dovtedy, kým je to potrebné na sledované účely. Nariadenie nestanovuje žiadnu konkrétnu minimálnu, ako ani maximálnu dobu uchovávania osobných údajov a túto si musí prevádzkovateľ nastaviť samostatne tak, aby to vyhovovalo jednak účelu ale aj primeranosti a proporcionalite s ochranou súkromia dotknutých osôb. V prípade ak je to technicky a organizačne možné, mal by prevádzkovateľ pristúpiť k anonymizácii údajov a ďalej využívať iba agregované a anonymizované údaje. Nariadenie pripúšťa dlhšiu dobu uchovávania údajov na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu či na štatistické účely v súlade s článkom 89 ods. 1 za predpokladu prijatia primeraných technických a organizačných opatrení vyžadovaných týmto nariadením na ochranu práv a slobôd dotknutých osôb.

V každom prípade by prevádzkovateľ mal spracúvanie obmedziť na striktné minimum (okrem prípadov, kedy dobu uchovávania stanovujú osobitné právne predpisy). Pre prípady overenia je vhodné stanovenú dobu pravidelne prehodnocovať, aktualizovať testy proporcionality a uchovávať záznamy o príkladoch, ktoré poukazujú na potrebu kratšej/dlhšej doby spracúvania.

2.1.6 Integrita a dôvernosť

Zásada zachovania bezpečnosti a ochrany osobných údajov vyjadrená najmä prostredníctvom zachovania ich integrity a dôvernosti dopĺňa všetky ostatné zásady najmä zdôraznením takého spracúvania, ktoré „zaručuje primeranú bezpečnosť osobných údajov, vrátane ochrany pred neoprávneným alebo nezákonným spracúvaním a náhodnou stratou, zničením alebo poškodením, a to prostredníctvom primeraných technických alebo organizačných opatrení“ (GDPR, Článok 5, ods. 1, písm. f)).

Opatrenia podporujúce integritu a dôvernosť vychádzajú už z podstaty minimalizácie údajov a ich uchovávania a nadväzujú na podmienky špecificky navrhnutej a štandardnej ochrany. Pri vyhodnocovaní primeranosti opatrení je potrebné implementovať najnovšie (state of the art) techniky, podmienky šifrovania

a kryptografie, autentifikácie ale aj fyzického zabezpečenia objektov. Pri stanovovaní opatrení by mali prevádzkovatelia vykonať analýzu rizík, posúdenie vplyvu na ochranu osobných údajov a testy proporcionality pri použití najnovších technických noriem a usmernení dozorných orgánov.

2.2 Posúdenie vplyvu na ochranu údajov

Ak typ spracúvania osobných údajov, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov (GDPR, Článok 27, ods. 1). S pokrokom v informačných technológiách sa každý rok automaticky spracúva čoraz viac osobných údajov. To je dôvod, prečo je potrebné prijať účinné, primerané a ekonomické bezpečnostné opatrenia na ochranu súkromia dotknutých osôb. Slepým uplatňovaním bezpečnostných opatrení bez hlbších znalostí o citlivosti takýchto osobných údajov nenaplní očakávania prevádzkovateľov. Na prekonanie tohto konfliktu očakávaní je potrebné si vytvoriť systém hodnotenia citlivosti osobných údajov ako nástroj na priradenie vhodných bezpečnostných opatrení podľa správnej úrovne citlivosti (Loveček, 2017).

Posúdenie vplyvu na ochranu údajov (DPIA: Data Protection Impact Assesment) je proces určený na opis spracovania, posúdenie nevyhnutnosti a proporcionality spracovania a na pomoc pri zvládaní rizík týkajúcich sa práv a slobôd fyzických osôb vyplývajúcich zo spracovania osobných údajov. DPIA je dôležitým nástrojom zodpovednosti, pretože pomáha prevádzkovateľom nielen splniť požiadavky GDPR, ale tiež preukázať, že boli prijaté príslušné opatrenia na zabezpečenie súladu s GDPR. Inými slovami, DPIA je proces budovania a preukazovania súladu (WP29, 2017).

Podľa GDPR, článok 35, ods. 3 posúdenie vplyvu na ochranu údajov sa vyžaduje najmä v prípadoch:

- systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu,

- spracúvania vo veľkom rozsahu osobitných kategórií údajov (napr. biometrické údaje) alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky,
- systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

Úradu na ochranu osobných údajov Slovenskej republiky (ÚOOÚ SR) na svojich webových stránkach zverejnil zoznam spracovateľských činností podliehajúcich posúdeniu vplyvu na ochranu osobných údajov Slovenskej republiky. Z pohľadu monitorovania a trasovania ide napríklad o (ÚOOÚ SR, 2019):

- spracúvanie lokalizačných údajov,
- monitoring práce zamestnanca na základe vážnych dôvodov vyplývajúcich z osobitnej povahy činnosti zamestnávateľa,
- spracovateľské operácie využívajúce nové alebo inovatívne technológie.

Z uvedeného vyplýva, že monitorovanie a trasovanie osôb v zdravotníckych zariadeniach podlieha posúdeniu vplyvu na ochranu údajov.

Podľa vyhlášky Úradu na ochranu osobných údajov Slovenskej republiky (Vyhláška ÚOOÚ SR č. 158/2018 Z.z.) dokumentácia na posúdenie vplyvu obsahuje:

- opis plánovaného spracúvania,
- posúdenie nevyhnutnosti a primeranosti v spojení s opatreniami na preukázanie súladu so zákonom,
- posúdenie rizika pre práva fyzickej osoby v spojení s opatreniami na riešenie rizík.

Opis plánovaného spracúvania je systematickým opisom spracovateľských operácií zameraných na povahu, rozsah, kontext a účely spracúvania osobných údajov, ktorý obsahuje najmä:

- účel spracúvania osobných údajov,
- opis posúdenia oprávnenosti záujmu prevádzkovateľa alebo tretej strany,
- opis vzťahu prevádzkovateľa a dotknutých osôb,
- podmienky, na ktorých základe dotknutá osoba môže primerane očakávať spracovateľské operácie s osobnými údajmi, ktoré sa jej týkajú,
- posúdenie primeranosti spracovateľských operácií a odôvodnenia prevahy záujmu prevádzkovateľa alebo tretej strany nad právami fyzickej osoby,
- zoznam alebo rozsah osobných údajov, ktoré sú predmetom spracúvania,

- zoznam alebo okruh príjemcov, ktorým sú osobné údaje poskytnuté,
- vymedzenie obdobia uchovávania osobných údajov.

Na zabezpečenie súladu so zákonom musí byť spracovateľská operácia vo vzťahu k účelu spracúvania osobných údajov nevyhnutná a primeraná. Nevyhnutnosť spracovateľskej operácie sa preukazuje jej posúdením vo vzťahu k požadovanému účelu spracúvania osobných údajov. Primeranosť spracovateľskej operácie sa preukazuje posúdením jej povahy, rozsahu a kontextu, ktorý musí zodpovedať účelu spracúvania osobných údajov. Príklad posúdenia nevyhnutnosti a primeranosti s monitorovacími systémami je uvedený v tabuľke (Tabuľka 2).

Tabuľka 6 Príklady posúdenia nevyhnutnosti a primeranosti spracovania osobných údajov pomocou monitorovacích a trasovacích systémov v zdravotníckych zariadeniach (Loveček, 2022)

Záznam o spracovateľskej činnosti	**Nevyhnutnosť spracúvania**	**Primeranosť spracúvania**
Monitorovanie a kontrola zamestnancov prostredníctvom kamerového systému	Spracúvanie osobných údajov je založené na oprávnenom záujme prevádzkovateľa. Pri predmetnej spracovateľskej činnosti neexistujú reálne alternatívy, ktoré by umožňovali dosiahnuť účel spracúvania (monitorovanie zamestnancov v rámci kontrolného mechanizmu) iným, porovnateľne efektívnym spôsobom, najmä za zohľadnenia rozsiahlosti priestorov prevádzkovateľov zdravotníckych zariadení. Monitorovanie zamestnancov je nevyhnutné nielen pre ich kontrolu ale aj pre prípadné preukazovanie právnych nárokov rôznych osôb (napríklad sťažnosti pacientov, prípadné konflikty s personálom,	Rozsah a spôsob spracúvania osobných údajov je primeraný k účelu spracúvania a k povahe prevádzkovateľa. Spracovanie predmetných osobných údajov je primerané na dosiahnutie oprávneného záujmu sledovaného prevádzkovateľom v postavení zamestnávateľa – poskytovateľa zdravotnej starostlivosti, na ktorého sa kladú povinnosti pri výkone zdravotníckych činností, zabezpečení dôvernosti a ochrany pacientov ako aj pri efektívnom poskytovaní svojich služieb.

	kontrola vykonaných úkonov a činností a pod.)	
Monitorovanie verejných priestorov prostredníctvom kamerového systému za účelom ochrany zdravia a života, bezpečnosti a prevencie kriminality	Spracúvanie osobných údajov je založené na oprávnenom záujme prevádzkovateľa. Pri predmetnej spracovateľskej činnosti neexistujú reálne alternatívy, ktoré by umožňovali dosiahnuť účel spracúvania (monitorovanie priestorov prístupných verejnosti) iným, porovnateľne efektívnym spôsobom, najmä za zohľadnenia rozsiahlosti priestorov prevádzkovateľov zdravotníckych zariadení.	Rozsah a spôsob spracúvania osobných údajov je primeraný k účelu spracúvania a k povahe prevádzkovateľa. Spracovanie predmetných osobných údajov je primerané na dosiahnutie oprávneného záujmu sledovaného prevádzkovateľom s ohľadom na zabezpečenie ochrany majetku a splnenia obmedzenia prístupu neoprávneným osobám do priestorov prevádzkovateľa.
Monitorovanie vozidiel prevádzkovateľa prostredníctvom GPS	Spracúvanie osobných údajov je založené na oprávnenom záujme prevádzkovateľa. Prevádzkovateľ môže vyžadovať informácie o aktuálnej polohe svojich vozidiel jednak na splnenie evidenčných povinností (napríklad evidencia jázd, prehľad spotreby a pod.) ale aj pre efektívne vyťaženie vozidiel a plánovania ich nasadenia. S ohľadom na výkon predmetnej spracovateľskej činnosti neexistujú reálne alternatívy, ktoré by umožňovali dosiahnuť účel spracúvania iným, porovnateľne efektívnym spôsobom.	Rozsah a spôsob spracúvania osobných údajov by mal byť obmedzený len na služobné vozidlá a nemal by byť nasadený bez predchádzajúceho upozornenia používajúcich zamestnancov. Monitorovanie by malo byť nasadené len pri zohľadnení pseudoanonymizačných techník a v prípade možnosti použitia služobných vozidiel aj na súkromné účely umožňovať vypnutie monitorovania v súkromnom čase.
Riadenie (monitorovanie) vstupov do vyhradených priestorov (napr.: priestory s vybranými chemickými látkami, liečivami, radiačnými zariadeniami pod.)	Spracúvanie osobných údajov je založené na oprávnenom záujme prevádzkovateľa ale aj zákonných požiadavkách na zabezpečenie kontrolovaných substancií alebo obmedzení prístupu do určitých priestorov.	S ohľadom na povahu chránených vecí a priestorov môže v tomto prípade ísť o rôzne organizačné alebo priestorové opatrenia, ktoré zaručia požadovanú mieru kontroly a evidencie. Toto môže s ohľadom na jednotlivé aplikácie obsahovať evidenčné listy, vstupné ID karty, školenia, riadenie kľúčovej politiky, kontrolu strážnou službou a pod.

	V každom prípade by rozsah osobných údajov mal byť zúžený na absolútne minimum a spracúvaný spôsobom, ktorý je neinvazívny.	
Riadenie, kontrola a logovanie prístupov k elektronickej zdravotníckej dokumentácií	Spracúvanie osobných údajov je založené na zákonných požiadavkách na zabezpečenie kontroly a evidencie prístupov do elektronickej zdravotníckej dokumentácie. Takéto opatrenia vyžadujú jednak osobitné právne predpisy ale aj potreba zabezpečenia dôvernosti a súkromia pacientov.	S ohľadom na povahu chránených informácií (elektronické údaje) pôjde v tomto prípade najmä o rôzne organizačné a technické opatrenia, ktoré zaručia požadovanú mieru kontroly a evidencie. Toto môže s ohľadom na jednotlivé aplikácie obsahovať opatrenia v oblasti riadenia prístupov (prideľovanie prístupových práv), požiadavky na heslovú politiku, neprenositeľnosť ID kariet, systémy na autentifikáciu a autorizáciu, vyhodnocovanie logov a podozrivých aktivít/prístupov a pod.
Monitorovanie a trasovanie zamestnancov za účelom ochrany zdravia a života	Spracúvanie osobných údajov je založené na výkone úloh vo verejnom záujme, napríklad v oblasti ochrany verejného zdravia a zabezpečení prevádzky zdravotníckych zariadení.	V prípade vyhlásenej mimoriadnej situácie môžu byť zavedené rôzne pravidlá a podmienky pre zachovanie fungovania zdravotníckych zariadení s ohľadom prevencie a ochrany zamestnancov pred nákazlivými chorobami. Konkrétne opatrenia a možnosti trasovania a monitorovania vyplývajú z technických možností prevádzkovateľa ako aj na základe požadovaných cieľov, ktoré by sa mali pravidelne preskúmavať a prehodnocovať (či trasovanie/monitorovanie poskytuje požadovanú úroveň prevencie a ochrany zamestnancov).
Monitorovanie a trasovanie hospitalizovaných pacientov za účelom ochrany zdravia a života	Spracúvanie osobných údajov je založené na výkone úloh vo verejnom záujme, napríklad v oblasti ochrany verejného zdravia a ochrany verejnosti pred nákazlivými chorobami. Príkladom podobného použitia by mohla byť aplikácia eKaranténa, ktorá bola zavedená do praxe ako prostriedok monitorovania dodržiavania karanténnych opatrení.	V prípade vyhlásenej mimoriadnej situácie môžu byť zavedené rôzne pravidlá a podmienky pre zachovanie a podporu verejného zdravia. Tieto opatrenia by mohli zahŕňať aj obmedzenia slobody pohybu a súkromia formou monitorovania a trasovania nakazených osôb alebo osôb s povinnou karanténou. Konkrétne opatrenia a možnosti trasovania a monitorovania vyplývajú z technických možností prevádzkovateľa ako aj na základe požadovaných cieľov, ktoré by sa mali pravidelne preskúmavať a prehodnocovať (či trasovanie/monitorovanie poskytuje

		požadovanú úroveň prevencie a ochrany verejného zdravia).
Monitorovanie a trasovanie pacientov ambulantnej starostlivosti	Spracúvanie osobných údajov je založené na súhlase dotknutých osôb. Príkladom by mohlo byť dobrovoľné zaradenie pacienta do kontrolnej skupiny pri výskume alebo náhrada ústavnej starostlivosti formou monitorovania v domácom prostredí.	Rozsah a spôsob monitorovania by mal byť jasne určený s ohľadom na požadované ciele. Dotknutá osoba by mala byť zrozumiteľne poučená o dosahoch a dôvodoch takéhoto spracúvania a mala by mať možnosť slobodne súhlasiť alebo odmietnuť takéto spracúvanie s reálnymi alternatívami, ktoré by neovplyvnili poskytovanie služby pre dotknutú osobu.

Pri posúdení nevyhnutnosti a primeranosti spracovateľskej operácie sa zohľadnia a odôvodnia všetky základné zásady spracúvania osobných údajov (zákonnosť, spravodlivosť a transparentnosť, obmedzenie účelu, minimalizácia údajov, správnosť, minimalizácia uchovávania, integrita a dôvernosť).

Posúdenie rizika pre práva fyzickej osoby prevádzkovateľ sa vykonáva z pohľadu dopadov na fyzickú osobu, pričom zohľadňuje najmä riziko súvisiace s náhodným alebo nezákonným poškodením, zničením, stratou, zmenou, neoprávneným prístupom a poskytnutím alebo zverejnením osobných údajov, ako aj s akýmkoľvek iným neprípustným spôsobom spracúvania, pričom sa identifikujú:

- hrozby a pravdepodobnosť ich výskytu,
- zraniteľnosti zneužiteľné hrozbami,
- riziká a pravdepodobnosť ich výskytu a závažnosť,
- dopady na práva fyzickej osoby v dôsledku straty integrity, dôvernosti a dostupnosti údajov,
- vysoké riziká pre práva fyzickej osoby, ak sa neprijmú opatrenia na zmiernenie rizika.

Riziko by sa malo posudzovať na základe objektívneho posúdenia, ktorým sa určí, či spracovateľské operácie obsahujú riziko alebo vysoké riziko (GDPR, Recitál 76).

Prevádzkovateľ následne musí prijať primerané opatrenia na zmiernenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany spracúvaných osobných údajov.

2.3 Test proporcionality

V prípade pokiaľ je spracúvanie osobných údajov založené na oprávnenom záujme prevádzkovateľa je potrebné spracovať test proporcionality. Cieľom testu proporcionality (alebo niekedy uvádzaným aj pod názvom balančný test) je vyhodnotenie, či oprávnený záujem, ktorý sleduje prevádzkovateľ neprevažuje nad záujmami alebo základnými právami dotknutých osôb, ktoré by si vyžadovali ochranu osobných údajov. Vychádzajúc z tejto definície uvedenej v Článku 6 odsek 1 f) Nariadenia GDPR je možné skonštatovať, že realizáciou testu proporcionality bude vyhodnotenie súboru otázok, ktoré zhodnotia záujmy všetkých zainteresovaných strán a vyhodnotenie koho záujem v danom prípade prevažuje. Hoci samotné Nariadenie GDPR vo svojich recitáloch obsahuje viaceré usmernenia alebo príklady, nie je možné vytvoriť jednoznačný zoznam oprávnených záujmov, pretože jednotlivé aspekty spracúvania osobných údajov budú v každom jednom prípade špecifické a ich vyhodnotenie má vyplynúť z testu proporcionality.

V recitáli 47 sa uvádza, že „Existencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie.“ Vo všeobecnosti by sa dalo uviesť, že test proporcionality by mal obsahovať všetky časti, ktoré sú relevantné pre opísanie oprávneného záujmu a zhodnotenie záujmov všetkých zainteresovaných strán.

V rámci identifikácie oprávneného záujmu by prevádzkovateľ mal opísať čo daným oprávneným záujmom sleduje, aký je jeho účel, vyhodnotenie legitímnosti a legálnosti daného záujmu. Takéto popísanie oprávneného záujmu je nevyhnutné, pretože využiť sa môže iba oprávnený záujem, ktorý má jasne daný, konkrétny a špecifický účel, ktorý neodporuje právnym predpisom (a teda je legálny) a je legitímny (je možné a primerané očakávať, že prevádzkovateľ bude takúto činnosť vykonávať). Pokiaľ je oprávnený záujem legálny a legitímny musí prevádzkovateľ ešte preukázať, že daný účel je nevyhnutný a nie je možné ho dosiahnuť inými spôsobmi (samozrejme pri zohľadnení primeraného úsilia, technických a organizačných možností a očakávaného výsledku spracúvania osobných údajov).

Pri posudzovaní záujmov zainteresovaných strán je v rámci testu proporcionality vyhodnocované či dotknuté osoby môžu primerane očakávať spracúvanie svojich osobných údajov na stanovený účel, aký je vzťah dotknutej osoby a prevádzkovateľa (najmä pre vylúčenie prípadných konfliktov záujmov alebo násilného zásahu do súkromia osoby z pozície nadradenosti), informácie o dopadoch spracúvania na dotknutú osobu aj s popisom prípadných rizík narušenia bezpečnosti takéhoto spracúvania, popis bezpečnostných, organizačných a iných aspektov spracúvania (najmä ak by mohli byť pre dotknutú osobu prekvapivé), zhodnotenie možností uplatnenia práv dotknutej osoby a splnenia zákonných povinností (napríklad v oblasti transparentnosti).

Pri zhodnotení testu proporcionality sa na základe uvedeného vyhodnotí aký vplyv má spracúvanie na každú zainteresovanú stranu, či je oprávnený záujem jasne identifikovaný a legálny, či nie je možné dosiahnuť stanovený účel inými vhodnejšími prostriedkami a pokiaľ z testu vyplynie, že záujmy alebo základné práva dotknutej osoby neprevažujú nad oprávneným záujmom prevádzkovateľa, môže pristúpiť k spracúvaniu osobných údajov.

Rovnako ako aj pri akomkoľvek inom spracúvaní osobných údajov, je oprávnený záujem potrebné neustále monitorovať a v prípade zmeny spracúvania alebo externých podmienok, záujmov alebo legislatívy, tieto oprávnené záujmy podrobiť aktualizácii a overeniu, či test proporcionality stále vychádza v prospech oprávneného záujmu prevádzkovateľa.

2.4 Posúdenie rizika pre práva a slobody dotknutých osôb a návrh opatrení na ich riešenie

Podľa GDPR, Článok 32 prevádzkovateľ musí prijať primerané technické a organizačné opatrenia s cieľom zaistiť úroveň bezpečnosti primeranú tomuto riziku so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účely spracúvania, ako aj na riziká s rôznou pravdepodobnosťou a závažnosťou pre práva a slobody fyzických osôb.

Podľa Zákona č.18/2018 Z.z., §78 ods. 11 a Vyhláška ÚOOÚ SR č.158/2018 Z.z., §5 ods. 3 prevádzkovateľ pri prijímaní bezpečnostných opatrení a pri posudzovaní vplyvu na ochranu osobných údajov postupuje primerane podľa medzinárodných noriem a štandardov bezpečnosti.

Manažment rizík je kľúčovým nástrojom pre systematické riadenie bezpečnosti informačných systémov. Dôkladná znalosť skutočných rizík v súvislosti s informačnými systémami rozhoduje o výbere a presadzovaní vhodných bezpečnostných opatrení, ktoré sú schopné znížiť možnosť výskytu, resp. rozsah negatívnych dopadov. Manažment rizík je preto základom pre každý systém manažérstva informačnej bezpečnosti. V súčasnosti existuje skupina medzinárodných štandardov zameraných na rôzne aspekty manažmentu rizík informačnej bezpečnosti v organizáciách:

- ISO 31000:2010 Risk management - Principles and guidelines: zásady a generické smernice pre manažérstvo rizík pre verejné, súkromné alebo štátne podniky, združenia, skupiny alebo jednotlivcov.
- ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements: požiadavky na vytvorenie, zavedenie, údržbu a stále zlepšovanie systému riadenia informačnej bezpečnosti v kontexte organizácie. Požiadavky na posúdenie a ošetrenie rizík informačnej bezpečnosti prispôsobených potrebám organizácie.
- ISO/IEC 27005:2011 Information technology - Security techniques -
- Information security risk management: odporúčania pre riadenie rizík bezpečnosti informácií.
- ISO/IEC 29100:2011 Information technology - Security techniques -
- Privacy framework: rámec ochrany osobných údajov, ktorý definuje aktérov a ich úlohu pri spracúvaní osobných údajov.
- ISO/IEC 29134:2017 Information technology - Security techniques –
- Guidelines for privacy impact assessment: návod pre proces posudzovania vplyvu na súkromie.

V kapitole boli popísané právne aspekty, ktoré vplývajú na spracúvanie osobných údajov, špecificky pri monitorovaní a trasovaní pohybu osôb. S ohľadom na povahu špecifických prevádzkovateľov (zdravotnícke zariadenia), použité moderné technológie, zhodnotenie rizík spracúvania a ochranu verejného záujmu je možné konštatovať, že v špecifických prípadoch bude možné takéto spracúvanie legálne vykonávať za splnenia všetkých zákonných podmienok a požiadaviek. Ale aj napriek možnosti využívať tieto moderné spôsoby monitorovania a trasovania pohybu osôb by sa malo k ich nasadeniu pristupovať nanajvýš opatrne a len v nevyhnutných prípadoch s použitím na vopred obmedzený čas.

3. Monitorovanie pohybu osôb a sledovanie kontaktov v zdravotníckych zariadeniach

Zdravotnícke zariadenia možno považovať za tzv.“crowded places“. Crowded places vyjadrujú preplnené miesta s vysokou koncentráciou osôb a s nízku, resp. obmedzenou možnosťou riadenia pohybu osôb. Ako príklad je možné uviesť nemocnice nadregionálneho významu, ktoré poskytujú ambulantnú a ústavno-preventívnu starostlivosť. Dennodenne navštívi takéto zariadenie množstvo ľudí s cieľom získať potrebnú zdravotnú starostlivosť, pričom nie je možné vylúčiť prípadnú infekčnosť niektorých osôb pohybujúcich sa v priestoroch daného zariadenia.

Monitorovanie pohybu osôb pohybujúcich sa v rámci areálu zdravotníckeho zariadenia sa môže stať významnou pomôckou pri vyhľadávaní kontaktov potvrdených prípadov. Sledovanie kontaktov je jedným z hlavných nefarmaceutických opatrení pre zabránenie šírenia infekcie (Filonets, 2021). Existujú viaceré štúdie popisujúce proces sledovania kontaktov (Alarabi, 2021). Podľa Eames (2003) autori považujú sledovanie kontaktov, po ktorom nasleduje liečba alebo izolácia, za kľúčové kontrolné opatrenie v boji proti infekčným chorobám. Ide o formu lokálne cielenej kontroly, ktorá má potenciál byť vysoko účinná pri riešení nízkeho počtu prípadov. Eames (2007) sledovanie kontaktov opisuje ako viacstupňový proces zahŕňajúci diagnostiku infikovaného človeka, spracovanie všetkých pravdepodobných kontaktov tohto človeka, identifikácia následne infikovaných a opakovanie celého procesu.

González-Cabañas (2021) uvádza, že aktuálne nasadené mobilné aplikácie na sledovanie kontaktov zlyhali ako efektívne riešenie v súvislosti s pandémiou COVID-19. Nakoľko sa nepodarilo prilákať počet aktívnych používateľov potrebných na dosiahnutie efektívnej prevádzky, výskumná komunita stojí pred výzvou nájsť nové spôsoby, ktoré povedú k účinným riešeniam na sledovanie kontaktov. Autori taktiež ponúkajú svoje vlastné riešenie na sledovanie kontaktov, ktoré využíva dostupné geolokačné informácie.

3.1 Využitie mobilných aplikácií na sledovanie kontaktov

Mobilné aplikácie nachádzajú široké uplatnenie na obmedzenia šírenia infekčného ochorenia. Aplikácie, ktoré umožnia spätne vystopovať s kým sa ich používateľ

stretol označila Európska komisia za veľmi prínosné. Európska komisia prijala 8. apríla 2020 Odporúčanie č. C(2020) 2296 pod názvom Commission Recommendation on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (Odporúčanie Komisie o spoločnom súbore nástrojov Únie pre využívanie technológií a údajov na boj proti kríze spôsobenej COVID-19 a jej prekonanie, najmä pokiaľ ide o mobilné aplikácie a využívanie anonymizovaných údajov o mobilite) (EC, 2020a). Cieľom tohto odporúčania bolo vytvoriť spoločnú koncepciu na úrovni EU z hľadiska využívania mobilných aplikácií, aby bolo možné čo najrýchlejšie prijímať účinné opatrenia obmedzovania sociálnych kontaktov, vystríhať pred kontaktmi, brániť im a sledovať ich v snahe obmedziť šírenie ochorenia COVID-19. V odporúčaní sú stanovené všeobecné zásady, ktorými by sa mal riadiť vývoj takéhoto súboru nástrojov, pričom hlavnou prioritou je dodržiavanie zásad ochrany súkromia a osobných údajov.

Sledovanie kontaktov je jedným z najvýznamnejších opatrení v boji proti infekčným ochoreniam z hľadiska zabránenia šírenia infekcie a ochrany verejného zdravia. Veľmi užitočným nástrojom na sledovanie kontaktov v boji proti týmto ochoreniam sú mobilné aplikácie. Nakoľko tieto aplikácie však pracujú s citlivými osobnými údajmi je potrebné, aby boli v súlade s ochranou súkromia a platnou legislatívou. Z tohto dôvodu existuje veľa obáv, súvisiacich s používaním mobilných aplikácií, týkajúcich sa ochrany súkromia a anonymity, ako aj právnych otázok a problémov s ochranou osobných údajov. Tieto sú v plnom rozsahu zahrnuté v dokumente „eHealth: Network Mobile applications to support contact tracing in the EU's fight against COVID-19 (eZdravie: Sieťové mobilné aplikácie na podporu sledovania kontaktov v boji EÚ proti COVID-19) a v príručke Európskej komisie Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection (Usmernenie k aplikáciám na podporu boja proti pandémii COVID 19 v súvislosti s ochranou údajov) (EC, 2020b).

Účelom sledovania kontaktov je prerušiť prenosové reťazce infekcie tým, že sa zabezpečí, aby osoby, ktoré boli v kontakte s infikovanou osobou, boli upozornené, že sú vystavené zvýšenému riziku infekcie a je potrebné prijať opatrenia na zabránenie prenosu na iné osoby. Európske centrum pre prevenciu a kontrolu chorôb (ECDC: European Centre for Disease Prevention and Control) spracovalo usmernenie pre sledovanie kontaktov pre zvládnutie väčšieho počtu prípadov s

využitím rôznych typov technológií a taktiež aj ľudských zdrojov (European Centre for Disease Prevention and Control, 2020a). Podľa ECDC bežné manuálne sledovanie kontaktov však musí naďalej pokračovať nakoľko mobilné aplikácie považujú len za doplnok, ktorý nenahrádza manuálne sledovanie. Pod pojmom sledovanie kontaktov sa rozumie celková stratégia verejného zdravia a činností zahrnuté do sledovania a skúmania kontaktov. O mobilných aplikáciách nemožno povedať, že vykonávajú „sledovanie kontaktov", ale skôr ide o „ sledovanie blízkosti" a „oznámenie o expozícii", t. j. sledovanie a upozorňovanie používateľov, ktorí boli v tesnej blízkosti s osobou, ktorá je tiež zahrnutá do sledovania kontaktov (European Centre for Disease Prevention and Control, 2020a).

Mobilné aplikácie sú softvérové aplikácie, ktoré využívajú inteligentné zariadenia, najmä smartfóny. Väčšinou sú určené na rozsiahlu a cielenú interakciu s webovými zdrojmi, ktoré spracúvajú údaje o blízkosti a iné relevantné informácie zbierané početnými snímačmi nachádzajúcimi sa v akomkoľvek inteligentnom zariadení a ktoré si dokážu vymieňať informácie cez mnohé sieťové rozhrania s inými pripojenými zariadeniami (EC, 2020b).

Od začiatku krízy spôsobenej ochorením COVID-19 boli vyvinuté vo svete rôzne mobilné aplikácie. Tieto aplikácie obvykle plnia tri základné funkcie (EC, 2020b):

- informovanie a poradenstvo pre občanov a uľahčenie organizácie následnej zdravotnej starostlivosti o osoby so symptómami, často v kombinácii s dotazníkom na samo - diagnostikovanie,
- varovanie ľudí, ktorí boli v blízkosti infikovanej osoby, s cieľom prerušiť reťazce nákazy a zabrániť opätovnému výskytu infekcií počas fázy opätovného rušenia obmedzení,
- monitorovanie a vynucovanie karantény infikovaných osôb, prípadne kombinované s funkciami na posudzovanie ich zdravotného stavu počas karantény.

Niektoré aplikácie sú prístupné širokej verejnosti, iné len uzavretým skupinám používateľov so zameraním na sledovanie kontaktov na pracovisku. Vo všeobecnosti účinnosť týchto aplikácií nebola vyhodnotená. Informačné aplikácie a aplikácie na kontrolu symptómov môžu byť užitočné na zvyšovanie informovanosti občanov. Podľa odborného stanoviska sa však aplikácie určené na informovanie a varovanie

používateľov javia pri prevencii šírenia vírusu ako najsľubnejšie, najmä ak sa vezme do úvahy aj to, že v obmedzenejšej miere zasahujú do súkromia.

Mobilná technológia na podporu sledovania kontaktov bola prvýkrát použitá v Singapure pod názvom „Trace Together“. Používanie tejto aplikácie bolo dobrovoľné. Aplikácia prostredníctvom Bluetooth zbiera údaje z iných zariadení, ktoré boli v tesnej blízkosti so zariadením používateľa. Ak má používateľ pozitívny test na COVID-19, aplikácia umožňuje ohrozených jednotlivcov informovať o tom, čo majú robiť.

V Európe ako aj v iných krajinách prebehlo niekoľko iniciatív na vývoj mobilných aplikácií na sledovanie kontaktov. Väčšina je založených na Bluetooth, ktoré umožňujú detekciu blízkosti, ale nie sledovanie polohy. Ostatné aplikácie sú založené na GPS technológii. Európska komisia a „Súbor nástrojov“, ktorý vytvorili členské štáty v spolupráci s Komisiou, uvádza, že „údaje o polohe nie sú potrebné a ani sa neodporúčajú na účely aplikácií na sledovanie kontaktov“ (eHealth Network, 2020).

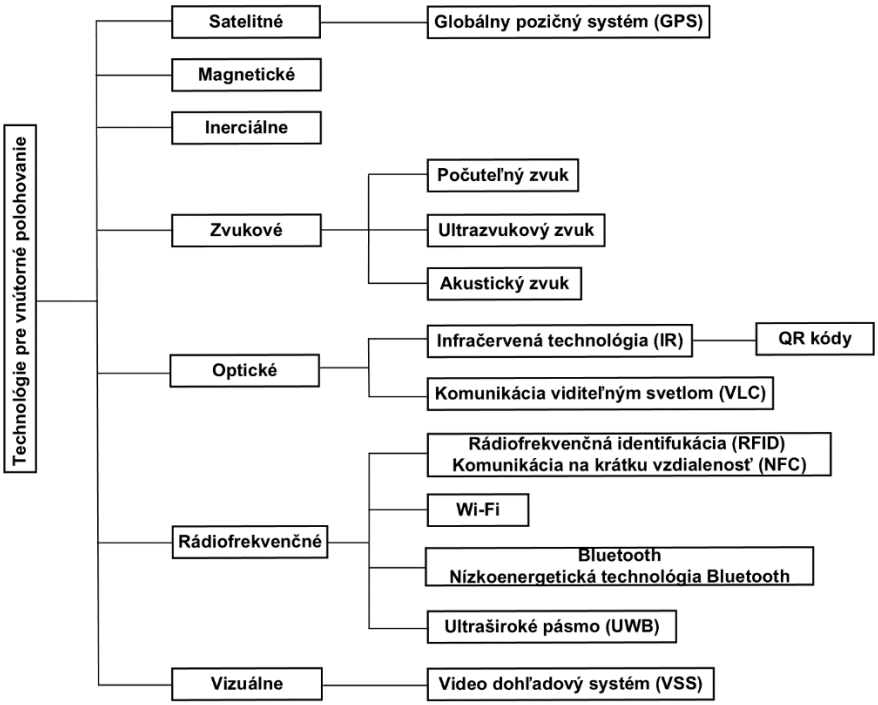
3.2 Technologické riešenia trasovania pohybu osôb

Trasovanie pohybu osôb je za určitých právnych a technických podmienok významným prvkom v oblasti bezpečnosti. Otázka trasovania pohybu osôb je na mieste, ak berieme do úvahy priestory, v ktorých sa vyžaduje dohľad na pohybom osôb, dohľad nad neoprávneným pohybom v chránenom objekte, dohľad nad pohybom osôb z hľadiska šírenia infekčnej choroby a ďalšie možné scenáre použitia. Napríklad, v čase pandémie COVID-19 je na mieste otázka monitorovania počtu osôb, ich pohybu (napr. v zdravotníckom zariadení), ich priblíženie k inej osobe na menej ako 1,5 a ž 2 m, či ich nadlimitné zhromažďovanie v určitom priestore (maximálna kapacita na plochu priestoru). Technické riešenia na trhu už existujú, resp. sú v rôznych fázach nasadenia, výskumu či vývoja.

Pre akademické, ale aj praktické riešenie vzniká otázka modelovania trasovania pohybu osôb v objektoch. Pomocou modelovania trasovania pohybu osôb, je možné získať teoretické poznatky, ktoré pomôžu vytvoriť a inštalovať systém monitorovania pohybu osôb v reálnom prostredí s menším počtom chýb alebo s efektívnejším rozmiestnením technických prvkov.

V ďalšom texte sú špecifikované vybrané technologické riešenia, pomocou ktorých je možné monitorovať a trasovať pohyb osôb a predmetov.

Existuje niekoľko typov technológií, ktoré je možné implementovať v rámci sledovania polohy a pohybu osôb a entít. Podľa pricípu fungovania poznáme satelitné, magnetické, inerciálne sensory, zvukové (počuteľný zvuk, ultrazvukový zvuk, akustický zvuk), optické, rádiofrekvenčné (WiFi, BLE, RFID, UWB) a vizuálne. Jednotlivé technológie určené na monitorovanie a trasovanie pohybu osôb a entít sú znázornené na obrázku 4.



Obrázok 4 Technológie umožňujúce monitorovanie a trasovanie osôb a predmetov (Intellectsoft US, 2020)(Beacon. What is ibeacon? A guide to beacons, 2021)

Magnetické, inerciálne, ultrazvukové či infračervené technológie sú využívané za účelom lokalizácie najmä v kombinácii s ďalšími technológiami. Väčšina uvedených technológií určených na lokalizáciu je vhodná pre použitie v rámci vonkajšieho i vnútorného prostredia. Technológia GPS je využiteľná v rámci prostredia, ktoré je pokryté signálom. Avšak použitie vo vnútorných priestoroch je častokrát obmedzené vzhľadom na nepriepustnosť signálov cez stavebné konštrukcie alebo prírodný terén. Technológie Ultrasound, RFID a NFC je možné implementovať najmä v interiéri budov. Medzi technológie umožňujúce sledovanie polohy objektov a osôb v reálnom čase patria GPS, IR, VLC, RFID, WiFi, Bluetooh, BLE, UWB a VSS. Niektoré

z technológií majú obmedzený dosah, v rámci ktorého sú schopné vysielacie a prijímacie zariadenia vzájomne komunikovať. Technológie ako Ultrasound, IR, NFC či QR kódy je možné charakterizovať ako technológie krátkeho dosahu. Dosah QR kódov závisí od veľkosti samotného kódu. Čím je väčší QR kód, tým je i čítacie zariadenie schopné kód naskenovať z väčšej vzdialenosti. RFID technológia rovnako ako WiFi, UWB a VSS umožňuje zariadeniam prijímať vysielané signály až do 50 m. Táto vzdialenosť je charakteristická najmä pre vysokofrekvenčné systémy. Pri nízkych frekvenciách klesá i komunikačná vzdialenosť. V porovnaní s WiFi, UWB a VSS je komunikačný dosah technológie Bluetooth a BLE nižší. Avšak komunikačný dosah približne 20-25 m je pre potreby monitorovania a trasovania pohybu entít v interiéri postačujúci. Pod pojmom Tracking rozumieme schopnosť technológie určovať polohu v priestore. Technológie RFID, NFC, WiFi a QR kódy z hľadiska lokalizácie poskytujú iba informácie o prítomnosti, respektíve neprítomnosti entity v danom priestore. Monitoring je možný na základe informácií o dobe prítomnosti entity v daných priestoroch. Avšak nie je možné určiť pohyb entity v priestore. Lokalizovať viac osôb a entít neumožňuje technológia NFC a QR kódy.

Je možné konštatovať, že z pohľadu dosahu technológie sa ako najvhodnejšie javia UWB a VSS. Avšak na rozdiel od vonkajšieho prostredia, pre vnútorné priestory nie je dôležité zameriavať sa na najväčší možný dosah technológie. Pre návrh a implementáciu vhodného vnútorného lokalizačného systému je rozhodujúcou charakteristikou predovšetkým schopnosť technológie určiť konkrétnu polohu osoby a entity v priestore. Nevýhodou implementácie systému VSS pre monitorovanie a trasovanie osôb je potreba zaistiť dostatočné pokrytie priestoru detekčnými charakteristikami kamier na úrovni rekognoskácie a taktiež účel využitia môže byť v konflikte s reguláciami na ochranu osobných údajov (GDPR, 2016). Technológiu BLE je možné použiť v exteriéri ako aj interiéri a umožňuje lokalizovať entity v reálnom čase. Komunikačná vzdialenosť pre prenos signálov je 25 m, čo pre vnútorné prostredie postačuje. Technológia je schopná entity trasovať, teda poskytovať informácie o polohe a pohybe v danom priestore. Vzhľadom na tieto skutočnosti technológia BLE má dobré predpoklady na monitorovanie a trasovanie pohybu osôb a predmetov v uzavretých priestoroch. Presnosť určovania polohy entít závisí od nastavenia celého systému, čo vytvára priestor pre množstvo výskumných úloh.

Cieľom výskumného projektu APVV-20-0457 Monitorovanie a trasovanie pohybu a kontaktu osôb v zdravotníckych zariadeniach, je vyvinúť prototyp technického riešenia, ktoré by umožňovalo monitorovať a trasovať osoby alebo predmety v uzatvorenom prostredí (napr. v komplexe budov s nízkou úrovňou GPS signálu). Systém by mal umožňovať určiť nie len polohu danej entity v konkrétnom priestore,

ale aj vzájomnú polohu jednotlivých entít, a to s požadovanou presnosťou závislou od praktickej aplikácie. Systém by mal byť nenáročný na napájanie, rušivé vplyvy prostredia (napr. Electromagnetic radiation, dym, teplota, prekážky, etc.) ako i prenositeľný a rýchlo použiteľný bez potreby napájania, rádovo na niekoľko dní. Systém by bol univerzálne využiteľný ako v bežnom prevádzkovom režime (napr. sledovanie dochádzky, logistické procesy sledovania pohybu tovarov), tak aj v režime vyvolanom mimoriadnou udalosťou alebo situáciou (monitorovanie a trasovanie osôb v objekte počas evakuácie z dôvodu požiaru, monitorovanie a trasovanie osôb z dôvodu šírenia infekčného ochorenia, ako napr. COVID-19).

Beacony je možné využiť v rôznych sférach a odvetviach, napríklad v rámci marketingu a obchodu, hotelierstva, kaviarní a reštaurácií, športu a štadiónov, múzeí, nákupných centier, kín a divadiel, letísk, bankovníctva, dopravy či zábavných parkov a mnoho ďalších. Je možné ich využiť na navigáciu v priestore, či na upozorňovanie na rôzne udalosti (Intellectsoft US, 2020). Bluetooth beacony využívajú Bluetooth Low Energy (BLE). Ide o rádiovú technológiu krátkeho dosahu. Je efektívna a užitočná, nakoľko využíva nízke úrovne energie. Beacony je možné napájať prostredníctvom pevného zdroja energie alebo použitím batérií (Beacon. What is ibeacon? A guide to beacons, 2021). iBeacon je technológia, ktorú vyvinula spoločnosť Apple v roku 2013. iBeacon funguje na princípe BLE a okrem iBeacon sú známe aj AltBeacon a Eddystone (Al-Alqusair, D. et al., 2019). Vnútorné určovanie polohy na báze Bluetooth 4.0 vyžaduje iba 3 ms na pripojenie a je schopné pokryť oblasť veľkú v priemere až 500 m2. Technológia iBeacon je charakteristická jednoduchou implementáciou, nízkou spotrebou energie a nízkou cenou. S dosahom niekoľko desiatok metrov dokáže presne určovať polohu v uzavretých priestoroch (Wang, Q., ae al., 2017).

3.3 Lokalizačné systémy v zdravotníctve

Podľa Gholamhosseini (2019) je výhodné z hľadiska nákladov a prínosov, monitorovať nielen zdravotnícky personál, či pacientov ale aj zdravotnícky materiál a vytvoriť tak nemocničný lokalizačný systém (ďalej NLS), ktorý lokalizuje osoby a materiál v reálnom čase (angl. real-time locating system).

Monitorovanie polohy pacientov, lekárov, zdravotníckeho personálu a zdravotníckeho majetku (materiálu) poskytuje manažérom v nemocniciach dostatočné množstvo informácii na efektívne riadenie chodu nemocnice. NLS systémy sú založené na tom, že zvýšia viditeľnosť prevádzkovú efektivitu pracovných tokov v nemocniciach a tak automatizovať niektoré nemocničné procesy (Sepehri, 2011). V čase pandémie COVID-19 (avšak nielen v tomto období) je NLS aj

preventívnym nástrojom na riadenie dištančných rozostupov osôb (personálu, pacientov či ostatných osôb) (Costs Tags - low H, High Medium, 2009).

Napríklad aplikácia U-Healthcare rieši monitorovanie starších osôb pred následkami tzv. abnormálnych stavov. Toto riešenie využíva technológiu rádiofrekvenčnej identifikácie (RFID) na presnú lokalizáciu a sledovanie. Systém umožňuje sledovanie pohybu osôb v reálnom čase. Okrem toho analyzuje ich umiestnenie v spojení s časovými úsekmi a dĺžkou času, počas ktorého zostávajú na rovnakom mieste (Kim, 2013). Belgická nemocnica v Ghente implementovala NLS založený na RFID. Účelom tohto systému bolo lokalizovať pacientov a nemocničný majetok v tzv. nevyhnutných podmienkach. Nemocnica posielala signály do nemocničnej Wi-Fi siete cez tzv. aktívne prvky. Každému zdravotníckemu majetku bol pridelený štítok, ktorý obsahoval jedinečnú informáciu o danom majetku a bolo možné ich vidieť prostredníctvom správ v mobilných telefónoch zdravotníckeho personálu (Bacheldor, 2007). Riešenia na báze kombinácie technológie Wi-Fi a RFID boli tiež implementované v ďalších nemocničných zariadeniach, napr. Luxembursku (Manzoor, 2016), Holandsku alebo Mexiku (Bacheldor, 2008). Rovnako Vilamovská (2009) navrhla metodiku použitia RFID siete zariadení, ktoré sú inštalované v sektore zdravotníctva.

Používanie náramkov s RFID štítkami pre pacientov bolo aplikované v Kanade, pričom princíp spočíva v poplachovom alarme, ktorý sa aktivuje v prípade prechodu pacienta s týmto náramkom cez dvere vybavené čítačkami RFID štítkov (Bacheldor, 2008). Presnú polohu pacienta v prípade opustenia nemocnice dokáže napr. systém X-Tag, ktorý je rovnako založený na technológii RFID (Vilamovska, 2009). Tento systém sa tiež používa na zabezpečenie identifikácie novorodencov či pacientov na detských oddeleniach. V Taliansku implementovali RFID štítok na urgentnom príjme prijatým pacientom, pričom sa RFID štítok spároval s nemocničnou databázou, ktorá obsahovala meno a priezvisko pacienta vrátane zdravotných informácií pacienta (Van Oranje-Nassau, 2009). V USA bol podobný systém rozšírený o posielanie informácií cez nemocničnú WiFi sieť prostredníctvom systému AeroScout. Tento systém na báze RFID štítkov prepája lokalizačné informácie s mapovým podkladom (Rain Alliance, 2022).

Očakávané výhody technológií založených napr. na technológii RFID sú najmä v produktivite, efektívnosti, zlepšovaní systému a starostlivosti o pacienta,

bezpečnosti a spokojnosti. Zlepšenie efektívnosti systému zahŕňa niekoľko prvkov súvisiacich s včasnosťou, bezpečnosťou, pracovným tokom, vysokým využitím kapacity, zníženými nákladmi pre pacienta a kontrolou procesu (Yazici, 2014).

Výhody efektívnosti pozostávajú z automatizácie procesov, zlepšenia produktivity a zníženia nákladov na pracovnú silu. Spokojnosť pacientov je významným ukazovateľom kvality zdravotnej starostlivosti. Napríklad implementácia NLS môže pomôcť znížiť medicínske chyby automatickým zabezpečením, že pacienti dostanú správny liek a dávku. Okrem toho možno NLS použiť na monitorovanie prostredia a pohybu pacientov v rámci zariadenia (Yazici, 2014).

Hlavnými dôvodmi implementácie NLS sú:

- Zvýšená produktivita, zvýšená efektivita a úspora nákladov vďaka: zníženým mzdovým nákladom, zníženiu zásob, minimalizácii strát zásob.
- Úspora nákladov vďaka zníženým stratám pri krádeži a zbytočnému plytvaniu.
- Zvýšená kvalita a bezpečnosť starostlivosti o pacienta znížením počtu chýb, skrátením času odozvy, zlepšením dodržiavania liekov pacientmi, zvýšením komunikácie a prístupu k údajom v reálnom čase medzi zdravotníckym personálom nemocníc, pacientmi, lekárňami, krvnými a orgánovými bankami.
- Lepšia podpora plánovania a kontroly.
- Zlepšenie pracovnej klímy a pracovných podmienok.
- Synchronizácia toku produktov (materiálu) a toku informácií.

Prijatie NLS systému v zdravotníckom zariadení predstavuje na druhej strane niekoľko výziev vrátane technologických, ekonomických, sociálnych a právnych a organizačných otázok. Tieto výzvy sú samozrejme častokrát na opačnom brehu, prečo neimplementovať NLS systém. Je len otázkou času, kedy lokalizačné systémy budú implementované v zdravotníckych zariadeniach aj na Slovensku, vrátane lokalizácie pacientov.

Záver

V období epidémií a pandémií pohyb osôb v mnohých zdravotníckych zariadeniach poskytujúcich zdravotnú starostlivosť nie je obmedzený a ani nie je možné ho úplne vylúčiť. Dennodenne navštívi takéto zariadenie množstvo ľudí s cieľom získať potrebnú zdravotnú starostlivosť, pričom nie je možné vylúčiť prípadnú infekčnosť niektorých osôb pohybujúcich sa v priestoroch daného zariadenia.

Monitorovanie a trasovanie pohybu osôb pohybujúcich sa v rámci areálu zdravotníckeho zariadenia sa môže stať významnou pomôckou pri vyhľadávaní kontaktov potvrdených prípadov. Nasadenie takéhoto systému prináša výhody ako napríklad zníženie možnosti šírenia infekčných chorôb, znižovanie nákladov súvisiacich s automatizovaným vyhľadávaním kontaktov, zvýšenie celkovej presnosti vyhľadávania kontaktov, zníženie liečebných nákladov štátu a neposlednom rade zvýšenie pripravenosti riešiť podobné krízové situácie aj v budúcnosti.

Implementácia monitorovacieho a trasovacieho systému v reálnom čase umožňuje zdravotníckym zariadeniam dosiahnuť ich ciele, ako je zlepšenie efektívnosti materiálu, zvýšenie spokojnosti pacientov a výrazné zníženie času a nákladov. Implementácia takýchto systémov v nemocniciach na Slovensku, čelí mnohým technologickým výzvam. Najdôležitejšími kritériami pre implementáciu niektorého riešenia sú ekonomické dôsledky a spokojnosť pacientov a zdravotníckeho personálu.

Ak sú správne pochopené potreby nemocníc, je možné predpokladať, že nemocničné zariadenia a pacienti ako používatelia, budú akceptovať a implementovať lokalizačné systémy vo svojich prevádzkach, tak ako sa tomu deje v zahraničí. Spomínané výhody predstavujú pre nemocnice významné benefity od bezpečnosti pacienta po znižovanie nákladov či efektivitu chodu nemocnice.

Súčasné lokalizačné, monitorovacie alebo trasovacie systémy predstavujú súhrn viacerých technológií, ktoré umožňujú sledovať rôzne predmety či osoby aj v uzavretých alebo vonkajších priestoroch. Ide napríklad o Global Position System (GPS), Radio-frequency identification (RFID), Near-Field Communication (NFC), Bluetooth Low Energy beacony, Video Survillinece Systems (VSS), Intruder and Hold-up Alarm Systems (I&HASs), WiFi, Bluetooth, atď. Nie všetky uvedené technológie sú však využiteľné v ľubovoľnom prostredí a na akúkoľvek aplikáciu.

Preto súčasným cieľom výskumných aktivít by malo byť vyvinúť informačný systém, ktorý by umožňoval monitorovať a trasovať osoby v uzatvorenom prostredí (napr. v zložitom komplexe budov s nízkou úrovňou GPS signálu). Tento systém by umožňoval určiť nie len polohu danej entity (človeka alebo veci) v konkrétnom priestore ale aj vzájomnú polohu jednotlivých entít, a to s presnosťou rádovo na niekoľko centimetrov. Systém by mal byť nenáročný na napájanie, rušivé vplyvy prostredia (rôzne spektrá elektromagnetického žiarenia, dym, vysoká teplota, fyzické prekážky, atď.) ako i prenositeľnosť a rýchlosť nasadenia. Systém by mal byť univerzálne využiteľný ako v bežnom prevádzkovom režime (napr. sledovanie dochádzky, logistické procesy súvisiace s evidenciou majetku, riadenie a kontrola prístupu do vyhradených priestorov, atď.), tak aj v režime vyvolanom mimoriadnou udalosťou, resp. situáciou (monitorovanie a trasovanie osôb v objekte počas evakuácie z dôvodu požiaru, monitorovanie a trasovanie osôb z dôvodu šírenia infekčného ochorenia, ako napr. COVID-19).

Použitá literatúra

Al-Alqusair, D. et al., 2019. “Measuring Patient Experience In Real Time Using iBeacon Technology”. TechnologicalCommunication. 230-238p. Dostupné na: https://www.researchgate.net/publication/334962025_Measuring_Patient_Experience_In_Real_Time_Using_IBeacon_Technology.

Alarabi, L., et al. 2021. TraceAll: A Real-Time Processing for Contact Tracing Using Indoor Trajectories. Information, 12, 202. Dostupné na: https://doi.org/10.3390/info12050202.

Bacheldor B. 2007. Belgium hospital combines RFID, sensors to monitor heart patients.

Bacheldor B. 2008. BlueTag Patient-Tracking Comes to North America. RFID Journal. Dostupné na: https://www.rfidjournal.com/articles/view?3906.

Baleľa, R., et al. 2008. Ekonomické hodnotenie v systéme zdravotnej starostlivosti. Fakmakoekonomika, roč. 5(6).

Boroš, M., Lettrich, E. 2020. Návrh monitorovacieho zariadenia pomocou platformy Arduino. In: Krízový manažment. Roč. 19, č. 2,s. 78-83.

Costs Tags-low H, High Medium. 2009. Real Time Location Systems, Clarinox Technologies Pty Ltd.

De Montjoye et al. 2013. Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports volume 3, Article number: 1376. 2013. Dostupné na: https://www.nature.com/articles/srep01376.

Eames, K. T. D., Keeling, M. J. 2003. Contact tracing and disease control. Proc. Biol. Sci. 270,

2565-2571. Dostupné na: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1691540/.

Eames, K.T.D. 2007. Contact tracing strategies in heterogeneous populations. Epidemiol. Infect 135(3), str.443-454. Dostupné na: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2870583/.

EC. 2020a. COMMISSION RECOMMENDATION of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data. Brussels, 8.4.2020.

C(2020) 2296 final. Dostupné na: https://ec.europa.eu/info/sites/default/files/recommendation_on_apps_for_contact_tracing_4. pdf.

EC. 2020b. Official Journal of the European Union. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection (2020/C 124 I/01). Dostupné na: https://eur-lex.europa.eu/legal-

content/SK/TXT/?uri=uriserv%3AOJ.CI.2020.124.01.0001.01.SLK&toc=OJ%3AC%3A202 0%3A124I%3ATOC.

European Centre for Disease Prevention and Control. 2020a. Resource estimation for contact tracing, quarantine and monitoring activities for COVID-19 cases in the EU/EEA. ECDC: Stockholm. Dostupné na: https://www.ecdc.europa.eu/sites/default/files/documents/COVID19-resources-for-contact-tracing-2-March-2020.pdf.

European Centre for Disease Prevention and Control. 2020b. Mobile applications in support of contact tracing for COVID-19. A guidance for EU/EEA Member States. Dostupné na:

https://www.ecdc.europa.eu/sites/default/files/documents/covid-19-mobile-applicationscontact-tracing.pdf.

eHealth Network. 2020. Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States, Version 1.0. Dostupné na:

https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

Filonets, T., et al. 2021. Investigation of the Efficiency of Mask Wearing, Contact Tracing, and Case Isolation during the COVID-19 Outbreak. J. Clin. Med, 10 (13), str. 2761. Dostupné na: https://doi.org/10.3390/jcm10132761.

GDPR. 2016. Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov). 2016. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/?uri=celex%3A32016R0679.

Gholamhosseini, L., Sadoughi, F., Safaei, A. 2019. Hospital Real-Time Location System (A Practical Approach in Healthcare): A Narrative Review Article. In: Iranian journal of public health, 48(4), str.593–602. PMCID: PMC6500521.

González-Cabanas, J., et al. 2021. Digital Contact Tracing: Large-Scale Geolocation Data as an Alternative to Bluetooth-Based Apps Failure. In: Electronics 2021, 10(9), str.1093. Dostupné na: https://doi.org/10.3390/electronics10091093.

Hudecová, I., Cyprichová, A., Makatura, I. 2018. Nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov-GDPR - Veľký komentár. 978-80-8155-077-5.

iBeacon. What is ibeacon? A guide to beacons. 2021. Dostupné na: http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/.

Intellectsoft US. 2020. "What Are Beacons and How Beacons Technology Works". Dostupné na: https://www.intellectsoft.net/blog/what-are-beacons-and-how-do-they-work/.

ISO/IEC 27005:2011 Information technology - Security techniques - Information security risk management: odporúčania pre riadenie rizík bezpečnosti informácií.

ISO/IEC 29100:2011 Information technology - Security techniques - Privacy framework: rámec ochrany osobných údajov, ktorý definuje aktérov a ich úlohu pri spracúvaní osobných údajov.

ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems. Requirements.

ISO/IEC 27002:2013 Information Technology - Security techniques - Information security management systems - Code of practice for information security controls: výber opatrení v rámci implementačného procesu systému manžérstva informačnej bezpečnosti.

ISO/IEC 29134:2017 Information technology - Security techniques – Guidelines for privacy impact assessment: návod pre proces posudzovania vplyvu na súkromie.

ISO 31000:2010 Risk management - Principles and guidelines: zásady a generické smernice pre manažérstvo rizík pre verejné, súkromné alebo štátne podniky, združenia, skupiny alebo jednotlivcov.

Jurkovičová, L. 2015. Ohodnocovanie komerčného potenciálu nových produktov a technológií. Studia commercialia Bratislavens. Dostupné na:

https://of.euba.sk/www_write/files/veda-vyskum/scb/vydane-cisla/201501/scb0115_Jurkovicova.pdf.

Kampová, K., Mäkka, K., Zvariková, K. 2019. Cost benefit analysis within organization security management. 19th International Scientific Conference Globalization and Its SocioEconomic Consequences 2019 – Sustainability in the Global-Knowledge Economy, 74. Dostupné na: https://10.1051/shsconf/20207401010.

Kim SC, Jeong YS, Park SO. 2013. RFID-based indoor location tracking to ensure the safety of the elderly in smart home environments. Pers Ubiquit Comput, 17(8), str. 1699–1707.

Lovecek, T., et al. 2017. Determination of Personal Data Sensitivity and Security Measures Assignment. 4th International Conference on Management Science and Management Innovation (MSMI 2017), Volume 31, p. 1-5.

Loveček, T., Magdolen, M. 2022b. Posúdenie vplyvu na ochranu osobných údajov pri monitorovaní a trasovaní osôb v zdravotníckych zariadeniach In: Riešenie krízových situácií v špecifickom prostredí, zborník príspevkov z 25. vedeckej konferencie s medzinárodnou účasťou. Žilina: Žilinská univerzita v Žiline, 2022. ISBN 978-80-554-1872-8. s. 316-329.

Lundkvist, J. 2005. Economic evaluation in the health care system. Department of economic evaluation in the health care system. Dostupné na: https://openarchive.ki.se/xmlui/bitstream/handle/10616/39993/thesis.pdf;sequence=1.

Ministerstvo zdravotníctva Slovenskej republiky. 2023. Organizácie v pôsobnosti ministerstva. Dostupné na: https://www.health.gov.sk/?organizacie-v-posobnosti-ministerstva

Manzoor, A. 2016. RFID applications in healthcare-state-of-the-art and future trends. Maximizing healthcare delivery and management through technology integration: IGI Global, 184–206. Dostupné na: https://doi.org/10.4018/978-1-4666-9446-0.ch012.

Ministerstvo zdravotníctva Slovenskej republiky. 2021. Metodický pokyn o predkladaní žiadostí o súhlas na použitie / poskytnutie finančných prostriedkov na investičné účely. Dostupné na: https://www.health.gov.sk/Zdroje?/Sources/dokumenty/mzsr/MPfin_prostriedky_investicne_ucely.pdf.

Pyrgelis, A., et al. 2017. Knock Knock, Who's There? Membership Inference on Aggregate Location Data. Cornell University: arXiv:1708.06145. Dostupné na: https://arxiv.org/pdf/1708.06145.pdf.

Rain Alliance. 2022. Healthcare Benefits of RAIN. Wakefield, USA.

Salomon, J. A., et al. 2021. The US COVID-19 Trends and Impact Survey: Continuous realtime measurement of COVID-19 symptoms, risks, protective behaviors, testing, and vaccination. Proceedings of the National Academy of Sciences of the United States of America 1800; 118 (51). DOI: 10.1073/pnas.2111454118.

Sassi, F. et al. 2001. Equity and the economic evaluation. Health Technology Assessment 5, (3).

Sepehri, M. M., Vahdat, D., Mollabagher, M. 2011. Designing of business information needs system of patients with improved health care in the surgical process using RFID technology Ministry of Science, Research and Technology. Thesis: Payam Noor University of Tehran.

Stobierski, T. 2019. How to do a Cost-benefit Analysis & why it is important,. Dostupné na: https://online.hbs.edu/blog/post/cost-benefit-analysis.

Usmernenia 4/2020 týkajúce sa lokalizačných údajov a iných nástrojov na sledovanie kontaktov v kontexte vypuknutia nákazy COVID-19. 2020. Dostupné na:

https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-uselocation-data-and-contact-tracing_sk.

Úrad na ochranu osobných údajov (ÚOOÚ SR). 2019. Metodika úradu Zoznam spracovateľských operácií podliehajúcich posúdeniu vplyvu na ochranu osobných údajov

Slovenskej republiky. Dostupné na:

https://dataprotection.gov.sk/uoou/sites/default/files/zoznam_spracovatelskych_operacii_ktor e_podliehaju_posudeniu_vplyvu.pdf.

Úrad pre verejné obstarávanie. 2020. Metodika kontroly hospodárnosti a efektívnosti vo verejnom obstarávaní. Dostupné na:

https://www.okruhlystol.sk/files/metodika_kontroly_hospodarnosti_vo_verejnom_obstarava ni_-_nku_-_uvo.pdf.

Úrad Žilinského samosprávneho kraja. 2023. Adresár zdravotníckych zariadení v zriaďovateľskej pôsobnosti ŽSK. Dostupné na: https://www.zilinskazupa.sk/sk/samosprava/urad-zsk/odbor-zdravotnictva/zdravotnicke-zariadenia-posobnosti-zsk/

Van Oranje-Nassau, C., et al. 2009. Study on the requierments and options for Radio Frequency Identification (RFID) application in healthcare. RAND technical report.

Vilamovska, A.M., et al. 2009. Study on the requirements and options for RFID application in healthcare. RAND technical report.

Yanan, D., et al. 2020. REACT: Real-Time Contact Tracing and Risk Monitoring via PrivacyEnhanced Mobile Tracking. Dostupné na: http://cs.emory.edu/site/aims/pub/da21icde.pdf.

Yap, K.Y.L., Xie, Q. 2020. Personalizing symptom monitoring and contact tracing efforts through a COVID-19 web-app. Infect Dis Poverty 9 (93). Dostupné na: https://doi.org/10.1186/s40249-020-00711-5.

Yazici H. J. 2014. An exploratory analysis of hospital perspectives on real time information requirements and perceived benefits of RFID technology for future adoption. Int J Inf Manage, 34(5):603–621.

Zákon č. 416/2001 Z.z. Zákon o prechode niektorých pôsobností z orgánov štátnej správy na obce a na vyššie územné celky

Zákon č. 576/2004 Z. z. o zdravotnej starostlivosti, službách súvisiacich s poskytovaním zdravotnej starostlivosti a o zmene a doplnení niektorých zákonov.

Zákon č. 578/2004 Z. z. o poskytovateľoch zdravotnej starostlivosti, zdravotníckych pracovníkoch, stavovských organizáciách v zdravotníctve a o zmene a doplnení niektorých zákonov.

Zákon č. 18/2018 Z.z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov.

Vyhláška Úradu na ochranu osobných údajov Slovenskej republiky č.158/2018 Z.Z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov.

Wang, Q., at al. 2017. An Indoor Positioning System Based on iBeacon. In: Pan, Z., Cheok, A., Müller, W., Zhang, M. (eds) Transactions on Edutainment XIII. Lecture Notes in Computer Science, vol 10092. Springer, Berlin, Heidelberg. Dostupné na: https://doi.org/10.1007/978-3-662-54395-5_22

World Health Organization. Monitoring and Evaluation of Contact Tracing. World Health Organization, 2021. Dostupné na: http://www.jstor.org/stable/resrep30107.16.

WP29, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. 2017.

Dostupné na:

file:///D:/Prevzat%C3%A9%20s%C3%BAbory/20171013_wp248_rev_01_en_D7D5A266FAE9-3CA1-65B7371E82EE1891_47711.pdf.