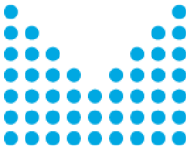


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MUNI

VLIV TECHNOLOGICKÝCH NÁSTROJŮ NA ÚSTAVNOST KRIZOVÝCH OPATŘENÍ OMEZUJÍCÍCH SVOBODU POHYBU

Souhrnná výzkumná zpráva zpracovaná v rámci projektu Omezení svobody pohybu: technologické možnosti a ústavněprávní limity (VI04000096)

Jakub Míšek, Anna Blechová, Michael Bátrla, Tereza Novotná, Ladislav Vyhnánek a Jakub Harašta

Masarykova univerzita, Právnická fakulta

říjen 2022

Tato souhrnná výzkumná zpráva byla vytvořena v rámci řešení projektu „Omezení svobody pohybu: technologické možnosti a ústavněprávní limity“ (VI04000096), který byl podpořen Ministerstvem vnitra ČR z Programu bezpečnostního výzkumu České republiky v letech 2015 až 2022.

Dostupnost zdrojů byla ověřena k 30. 9. 2022, pokud není u konkrétního zdroje uvedeno jiné datum.

Obsah

Manažerské shrnutí

Tato souhrnná výzkumná zpráva představuje druhý výstup projektu Omezení svobody pohybu: technologické možnosti a ústavněprávní limity (VI04000096), který se zabývá omezeními svobody pohybu, ke kterým dochází v rámci omezujících opatření směřujících ke zvládání krizí způsobených biologickými agens a toxiny. Tyto nefarmakologické intervence představují užitečný nástroj, nicméně vzhledem k jejich zásahu do práv a svobod jednotlivců se při jejich implementaci nelze omezit pouze na hodnocení jejich efektivnosti. V úvahu je nutné brát také jejich ústavněprávní a lidskoprávní dopady.

Prvním cílem této výzkumné zprávy bylo zmapovat trendy ve využívání technologických nástrojů v návaznosti na řešení krize způsobené šířením koronaviru SARS-CoV-2 v rámci stálých členů G20 v období od 1. ledna 2020 do 30. června 2021. Vědomi si limitů tohoto přístupu jsme následně provedli také dodatečnou rešerši bez geografického omezení pro období od 1. července 2021 do 31. srpna 2022. Využívané technologické nástroje byly následně rozděleny do skupin na základě účelů, ke kterým byly využity.

Druhým cílem této výzkumné zprávy bylo vytvoření vodítek, která pro jednotlivé skupiny technologických nástrojů usnadní vyhodnocení proporcionality jejich nasazení. Test proporcionality je sice možné provést až v konkrétním kontextu nasazení příslušné technologie za určitým účelem. Námi zpracovaná vodítka však umožní strukturovat hodnocení proporcionality s přihlédnutím k fázi krize a identifikují lidskoprávně relevantní parametry v rámci jednotlivých skupin technologických řešení.

Hlavním poznatkem z přehledové analýzy je možnost rozdělit technologické nástroje na pět základních typů (dva z nich s různými variantami) sledujících konkrétní cíle v podobě:

1. Trasování kontaktů s variantami využívajícími (i) protokol Bluetooth, (ii) zaznamenávání pohybu pomocí GNSS, (iii) zaznamenávání pohybu s využitím provozních a lokalizačních údajů, a (iv) jiný sběr a následné předávání informací orgánům veřejné správy
2. Statusové certifikáty
3. Bezkontaktní služby

4. Informování a edukace veřejnosti
5. Dohled a vynucování omezujících opatření s variantami využívajícími (i) neanonymizované provozní a lokalizační údaje, (ii) anonymizované provozní a lokalizační údaje, (iii) mobilní aplikace, (iv) jiné prostředky dohledu (např. náramky), (v) bezpilotní prostředky, a (vi) kamerové systémy.

V rámci těchto typů jsme pak identifikovali technologie, které nejsou za žádných okolností vhodné k nasazení z důvodu jejich zásahu do jádra práva na ochranu soukromí a osobních údajů. Jedná se o:

1. Trasování s využitím provozních a lokalizačních údajů
2. Využití neanonymizovaných provozních a lokalizačních údajů za účelem dohledu nad dodržováním omezujících opatření a jejich vynucování
3. Využívání automatického rozpoznávání obličejů (a dalších biometrických údajů) kamerami umístěnými na bezpilotních prostředcích
4. Plošné nasazování dronů za účelem dohledu nad dodržováním omezujících opatření a jejich vynucování
5. Využívání automatického rozpoznávání obličejů (a dalších biometrických údajů) statickými kamerovými systémy
6. Plošné sledování statickými kamerovými systémy sledujícími pohyb konkrétních vozidel prostřednictvím automatického rozpoznávání registračních značek

Nasazením ostatních technologií je dle našeho názoru možné v rámci konkrétního kontextu podepřít mimořádná opatření omezující svobodu pohybu. V důsledku jejich nasazení je totiž možné za určitých okolností efektivněji vymáhat existující opatření omezující svobodu pohybu bez neproporcionálního zásahu do práva na ochranu soukromí a osobních údajů. Vždy je však nutné vést v patrnosti, že test proporcionality je vázán na okolnosti konkrétní situace. Výsledky této výzkumné zprávy tak představují námi identifikované relevantní faktory a umožňují případnou diskuzi při zavádění či posuzování zásahu nástrojů strukturovat.

O projektu

Projekt Omezení svobody pohybu: technologické možnosti a ústavněprávní limity (VI04000096) se, v nejširší rovině, zabývá omezeními svobody pohybu, ke kterým dochází v rámci opatření směřujících ke zvládání krizí způsobených biologickými agens a toxiny.[1] Omezení svobody pohybu totiž představuje základní nefarmakologický nástroj, který má stát ve vztahu k těmto hrozbám k dispozici.[2] Cílem těchto opatření je zamezit jednotlivcům ve vstupu do vymezené oblasti, vymezenou oblast opustit nebo se v jejím rámci pohybovat (například stanovení zákazu opouštět obydlí).

Takováto omezení jsou při zvládání krizových situací účinná.[3] Představují však zásah do práv a svobod jednotlivců, kterých se týkají. Při přijímání opatření je tak nutné, kromě jejich faktické účinnosti, vést v patrnosti také ústavněprávní a lidskoprávní rozměr. Snaha o rychlé a efektivní zvládnutí krizové situace skrze přijímání omezujících opatření bude s největší pravděpodobností vždy do určité míry v konfliktu s běžně dodržovanou úrovní lidských práv.[4]

Celosvětové šíření koronaviru SARS-CoV-2 od počátku roku 2020 poskytlo rozsáhlou datovou bázi pro komplexní zmapování opatření směřujících k omezení pohybu v různých zemích. Některé státy mají z minulosti zkušenosti s nutností řešit šíření různých

[1] Tyto termíny jsou pro potřeby českého právního řádu vymezeny v §2 písm. a) (biologické agens) a písm. b) (toxin) zákona č. 281/2002 Sb., o některých opatřeních souvisejících se zákazem bakteriologických (biologických) a toxinových zbraní.

[2] Český pandemický plán explicitně zmiňuje, že nefarmakologická opatření je nutné zařadit vzhledem k možné omezené kapacitě a problematické časové dostupnosti farmakologických metod. Jakkoli je pandemický plán zaměřen zejména na chřipkové viry, sleduje stejnou logiku. V nefarmakologických opatřeních (důsledné mytí rukou, dobrovolná izolace nemocných, efektivní zjišťování kontaktů, omezení cestování hromadnými prostředky, omezení masového shromažďování lidí) spatřuje zejména nástroj pro získání času v úvodní fázi nastupující pandemie – tento čas má být využit k získání více údajů o průběhu a chování onemocnění způsobeného pandemickým virem a k vývoji pandemické vakcíny.

Viz Pandemický plán České republiky, 2011, s. 11.

[3] Viz například DEHNING, Jonas, Johannes ZIERENBERG, F. Paul SPITZNER a kol. Inferring change points in the spread of COVID-19 reveals the effectiveness of interventions. *Science*, 2020, sv. 369, č. 6500, eabb9789 nebo FLAXMAN, Seth, Swapnil MISHRA, Axel GANDY a kol. Estimating the effects of non-pharmaceutical interventions on COVID-19 in Europe. *Nature*, 2020, sv. 584, s. 257–261.

Viz také PERRA, Nicola. Non-pharmaceutical interventions during the COVID-19 pandemic: A review. *Physics Reports*, 2021, sv. 913, s. 1–52.

[4] V nejobecnější rovině k tomuto směřuje i český pandemický plán, který požaduje zajištění etičnosti pandemické odpovědi. Viz Pandemický plán České republiky, 2011, s. 6.

biologických agens, zejména s přihlédnutím k šíření koronaviru SARS-CoV, paramyxoviru spalniček nebo filoviru ebola. SARS-CoV-2 se stal biologickým agens, který nám umožňuje zkoumat rozdíly v přístupech k řešení rozsáhlé krize prostřednictvím omezování svobody pohybu a také využívání technologií ke kontrole a vynucování těchto opatření.

Hypotézou projektu je, že vhodným využitím technologických prostředků (například nástrojů pro vyhodnocování rizikových kontaktů nebo neinvazivního sledování pohybu) a cílených (místně lokalizovaných) opatření lze pnutí požadavku na efektivní zvládnutí krize a požadavku na dodržování standardu lidských práv zmírnit. Cílem projektu pak je identifikace technologických možností využitelných k zajištění souladu opatření směřujících k omezení pohybu s ústavním pořádkem.

Předmět zprávy

Tato výzkumná zpráva představuje přehled technologických nástrojů využitých při řešení krize související se šířením koronaviru SARS-CoV-2. Ve výzkumné zprávě si klademe za cíl předložit vícepřípadovou studii technologických prostředků využitých ve snaze zabránit šíření SARS-CoV-2 v rámci stálých členů uskupení G20.

Na základě případových studií identifikujeme skupiny technologických prostředků, které byly v rámci stálých členů uskupení G20 využity. Následně hodnotíme ústavněprávní limity jejich použití. Identifikujeme okolnosti, za kterých je využití těchto nástrojů nutné považovat za neproporcionální v důsledku jejich zásahu do práva na ochranu soukromého a rodinného života a práva na ochranu osobních údajů. Předkládáme také vodítka pro provedení testu proporcionality s přihlédnutím k typizovaným technologickým nástrojům a úloze, kterou mohou hrát v různých fázích krize související se šířením koronaviru SARS-CoV-2 (nástup agens; lokalizované šíření agens; nelokalizované šíření agens; návrat k běžnému chodu společnosti).

Současný stav poznání v České republice je logicky omezený zejména nedostatečným časovým a emocionálním odstupem od pandemie. Podobný dopad pak má absence racionálního zahraničního srovnání. Opatření, která byla v České republice vyhlášena, se bezprostředně dotýkala každého z nás. Diskuse o vhodnosti a účinnosti právních opatření (například zákaz pohybu usnesením vlády č. 85/2020 Sb.) i případných technologických nástrojů (například soubor opatření v rámci tzv. Chytré karantény) tak často probíhaly bez jejich zasazení do širšího (globálního) kontextu.

Klíčovou metodou využitou v rámci přípravy této výzkumné zprávy je kvalitativní analýza technologických prostředků využitých stálými členy G20 při řešení krize způsobené šířením SARS-CoV-2 a navázané zmapování ústavněprávních limitů jejich použití na abstraktní úrovni.

1. Úvod

V rámci snah o zvládnutí krize způsobené šířením koronaviru SARS-CoV-2 došlo k využití nejrůznějších technologických prostředků. Snahu s pomocí technologií podepřít trasování nakažených, šířit osvětu či dokázat, že byl jednotlivec negativně testován či v pozdější fázi pandemie očkován, rámovala konstantní obava o ochranu soukromí a osobních údajů. Této formě pozornosti se nevyhnuly ani aplikace tolik známé českým občanům, ať už se jedná o trasovací aplikaci eRouška či validační dvojici aplikací čTečka/Tečka.

Naše první výzkumná zpráva zmapovala opatření využitá pro řešení pandemie v rámci zemí G20 v období od 1. ledna 2020 do 30. června 2021.[5] Ve většině států sledované populace došlo ve sledovaném období k nasazení nějakých technických nástrojů. Ačkoli se jejich sofistikovanost i promyšlenost jejich použití dramaticky odlišovaly, trend snahy podepřít opatření omezující svobodu pohybu technologiemi byl jasný. Tím se však do diskuze o lidskoprávních dopadech omezujících opatření dostávají další práva – zejména právo na ochranu soukromí a ochranu osobních údajů.

Klasickým nástrojem pro hodnocení dopadů do těchto základních práv je test proporcionality. Ten je však nezbytné provést až v konkrétním případě. Ústavní soud k tomu v minulosti uvedl, že test proporcionality není možné ani ze strany zákonodárce provést abstraktně tak, aby komplexně obsáhl všechny konkrétní situace.[6] To však neznamená, že je přípustné rezignovat na jakoukoli snahu poskytnout pro uvažování o proporcionalitě či neproporcionalitě technologických nástrojů vodítka a identifikovat relevantní parametry.

Prvním cílem této výzkumné zprávy je zmapování trendů ve využívání technologických nástrojů v návaznosti na řešení krize způsobené šířením koronaviru SARS-CoV-2 v rámci stálých členů G20 v období od 1. ledna 2020 do 30. června 2021. Vzhledem k limitům spojeným s tímto přístupem jsme také přistoupili k dodatečné rešerši bez geografického

[5] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021.

[6] Viz nález Ústavního soudu ze dne 17. 10. 2007, sp. zn. IV. ÚS 1378/16.

omezení pro období od 1. července 2021 do 31. srpna 2022. Využívané technologické nástroje jsme pak rozdělili do skupin na základě účelů užití, které byly pozorovány.

Druhým cílem této výzkumné zprávy bylo vytvoření vodítek, která pro jednotlivé skupiny technologických nástrojů usnadní vyhodnocení proporcionality jejich nasazení. Test proporcionality je sice možné provést až v konkrétním kontextu nasazení příslušné technologie za určitým účelem. Námi zpracovaná vodítka však umožní strukturovat hodnocení proporcionality s přihlédnutím k fázi krize a identifikují lidskoprávně relevantní parametry v rámci jednotlivých skupin technologických řešení.

Po úvodní části, která v kapitolách 1.1 a 1.2 popisuje metodologii a limity, následuje část věnovaná přehledu technologií používaných ke zvládání pandemie (kap. 3.1) a následně je představována typologie využitých technologií (kap. 3.2). V další části formulujeme vodítka pro proporcionální nasazení analyzovaných technologií (kap. 4). Následují závěry zprávy (kap. 5).

1.1. Metodologie

Pro vypracování předkládané výzkumné zprávy byly využity textově analytické metody normativní právní vědy,[7] potažmo právní hermeneutiky.[8] Předkládaná výzkumná zpráva obsahuje shromážděná data o využívaných technologických řešeních (kap. 3), jejich analýzu (kap. 4) a diskusní závěr (kap. 5). S variantami využívaných technologických řešení pracujeme na abstraktní technické úrovni v tom smyslu, že neuvažujeme konkrétní společenský a kulturní kontext, ve kterém jsou daná technologická řešení nasazována. Záměrně je izolujeme tak, aby bylo možné pojednat o daném technologickém řešení bez nutnosti jeho okamžitého právního hodnocení v kontextu (právě kulturním či společenském), ve kterém bylo nasazeno. Slouží nám tak primárně jako inspirace pro vytvoření základní typologie nasazených technologických řešení v závislosti na jejich

[7] Viz SMITS, Jan M. *The mind and method of the legal academic*. Cheltenham, UK: Edward Elgar, 2012, s. 58 a následující. Také HOECKE, Mark Van. Legal Doctrine: Which Method(s) for What Kind of Discipline? In: HOECKE, Mark van, (ed.). *Methodologies of legal research: which kind of method for what kind of discipline?* Oxford, Portland: Hart, 2011, s. 1–18.

[8] Viz HLOUCH, Lukáš. *Teorie a realita právní interpretace*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011, s. 78. Dále HOLLÄNDER, Pavel. *Filosofie práva*. Plzeň: Čeněk, 2012, s. 289 a následující.

účelu. S touto inspirací následně pracujeme pro hodnocení případných zásahů do dalších práv.

Výzkumná zpráva přímo vychází z poznatků první výzkumné zprávy.[9] Sesbíraná data o využívaných technologických řešeních aplikovaných státy G20 (kap. 3) se tak vztahují na období od 1. ledna 2020 do 30. června 2021. Ze států G20, jejichž přístup k řešení pandemie byl popsán v první výzkumné zprávě,[10] jsme do této výzkumné zprávy nezahrnuli ty, které nepřinesly žádné typově nové technologické řešení. Cílem této výzkumné zprávy není podat kvantitativní analýzu četnosti ve využívání různých druhů technologií, ale získání kvalitativního přehledu možných variant nasazení.

Námi zvolená kombinace geografického a časového vymezení s sebou nese riziko, že do výzkumu nebyl zařazen nějaký zásadní typ technologie, který se v daném časovém období a v daném vzorku zemí nevyskytnul. K mitigaci tohoto rizika byla provedená dodatečná rešerše k datu 31. srpna 2022. Rešerše byla provedena bez geografického omezení a byla vedena na úrovni odborných článků a zdrojů, ale také v rovině článků populárně naučných a zpravodajských. Tato dodatečná rešerše neukázala na typově nové varianty technologií, které by nebyly zařazeny již v původním sledovaném období a v původně sledované populaci států. Přinesla nicméně několik aktualizací užití technologických nástrojů v zemích G20, což je v této zprávě reflektováno (kap. 3). Zároveň však, z důvodu absence typově nových variant užívaných technologií, není této dodatečné rešerši věnována samostatná kapitola.

Základním metodologickým východiskem pro hodnocení možností a limitů nasazení jednotlivých technologických řešení je test proporcionality. Také v tomto směru tak předkládaná výzkumná zpráva navazuje na závěry první zprávy.[11] V této zprávě pracujeme s hranicemi, které vymezují právo na ochranu soukromí a právo na ochranu osobních

[9] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021.

[10] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 14–115.

[11] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 116–139.

údajů, protože právě s těmito právy jsou užité technologie nejčastěji v kolizi. Na druhou stranu je nutné zdůraznit, že není v možnostech této výzkumné zprávy nabídnout komplexní vypracování testu proporcionality pro konkrétní případy případné aplikace analyzovaných technologických řešení (viz kap. 1.2). Test proporcionality je totiž nutné vždy provést až v konkrétním případě.[12] Z toho důvodu analýza (kap. 4) neobsahuje konkrétní finální řešení, ale představuje v obecnější rovině efekty hodnocených typů technologických řešení na průběh testu proporcionality.[13] Test proporcionality při aplikaci technologických řešení bude nutně zahrnovat porovnání více chráněných práv a zájmů najednou. Na jedné straně se bude obvykle nacházet zásah do práva na soukromí a osobních údajů. Na straně druhé pak kombinace zabránění zásahu do práva na svobodu pohybu a zajištění veřejného zájmu na zvládnutí pandemie. Kapitola 4 tak nabízí vodítka, která mají usnadnit rozhodování o možnostech nasazen různých technologií pro zvládání pandemie.

U každého typu technologií je hodnocena zejména (i) přítomnost kolize s jinými právy, (ii) možné varianty naplnění vymezeného účelu a jejich dopady na jednotlivá základní práva, a (iii) vliv nasazení technologického řešení v různých časových úsecích průběhu pandemie.

[12] Ústavní soud judikoval, že abstraktní provedení testu proporcionality, které by komplexně obsáhlo všechny konkrétní situace, není možné ani ze strany zákonodárce. Naopak je nezbytné nechat volnost hodnocení v konkrétních případech. Viz např. nález Ústavního soudu ze dne 17. 10. 2017, sp. zn. IV. ÚS 1378/16.

[13] Takovým efektem může být např. snížení dopadů opatření vedoucích k omezení svobody pohybu a tím pádem umožnění jejich průchodu testem proporcionality. Dopady však mohou být i negativní, například v podobě zásahu do jiného práva (zejm. práva na soukromí a ochranu osobních údajů).

1.2. Limity

S metodologickým přístupem, který jsme při přípravě této výzkumné zprávy zvolili, se pojí několik limitů.

První skupina limitů souvisí s přímým navázáním na závěry první výzkumné zprávy.[14] Vzhledem k úzké návaznosti je možné předpokládat, že se původně identifikované limity[15] projeví i v této výzkumné zprávě. Jedná se zejména o geografické a časové omezení oblasti pro sběr dat o užívaných technologiích. Tento limit jsme adresovali zahrnutím rešerše odborných i popularizačních zdrojů ke 31. srpnu 2022. I v tomto případě však zůstává limitem, že jsme čerpali zejména z anglickojazyčných zdrojů. Ty nemusí obsahovat všechny informace nebo v nich tyto informace mohou být z nejrůznějších důvodů zkreslené.

Druhý limit se týká zaměření této zprávy na technologie, které se objevily a byly využívány specificky pro zvládnutí pandemie a které měly potenciál snižovat míru zásahu do práva na svobodu pohybu. Mimo záběr tak zůstaly medicínské technologie, které napomohly k vývoji efektivních testů, vakcín a léků, jakkoliv byly tyto pro zvládnutí kritické fáze pandemie zcela zásadní. Přestože tak specifická technologie pro efektivnější testování na přítomnost specifických agens může sloužit k přesnějšímu a včasnému rozpoznání infikovaných osob (a sekundárně tak přispět k mírnějším a cílenějším omezujícím opatřením), nejedná se o její primární účel užití. Takováto technologie tak leží mimo rozsah našeho zájmu.

Třetí limit spočívá v námi zvoleném přístupu k identifikovaným technologiím. Jejich využití a hranice ústavnosti analyzujeme v obecné rovině. Mimo záběr této zprávy tak leží část konkrétních technických a implementačních detailů, které ale budou mít v konkrétních případech vliv na výsledek testu proporcionality. Tento limit je částečně vlastní testu proporcionality jako mechanismu, je však nutné ho zmínit.

---

[14] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 140–144.

[15] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 12–13.

2. Ústavní mantinely práva na soukromý a rodinný život

2.1. Právo na soukromí a jeho limity

Právo na soukromí je považováno za velmi obtížně vymezitelné, o čemž svědčí i neutuchající akademický zájem o jeho systematizaci. Z těch nejzásadnějších je možné vyjmenovat práce Warrena s Brandeisem,[16] Westina,[17] Clarka[18] nebo Soloveho.[19] Mimořádně kvalitní typologii (nástroj pro systematickou deskripci a následnou analýzu), která mapuje pojem soukromí v celé jeho šíři, nabídl autorský tým vedený Bert-Jaap Koopsem.[20] Z této studie vycházíme při popisu různých oblastí soukromí, do kterých může být zasaženo využíváním technologických prostředků pro zvládání pandemie. Činíme tak ze tří hlavních důvodů. Prvním důvodem je aktuálnost této typologie, která byla publikována v roce 2016. Druhým důvodem je vhodná provazba typologie s metodologickým uchopením tohoto textu. Při vytváření typologie autoři vycházeli z právní úpravy a ústavních tradic devíti států včetně České republiky.[21] Jejich závěry o struktuře práva na soukromí jsou tak pro potřeby této zprávy přímo použitelné. Třetím důvodem je pak z našeho pohledu samotná struktura typologie, která zahrnuje koncept informačního soukromí. Ten umožňuje velmi jednoduše popsat a zohlednit komplexní (a specifický) dopad moderních technologií.

Koops a kol. ve svém textu představili devět dimenzí soukromí, z nichž osm představuje konkrétní segmenty soukromí a devátá kategorie je překrývá. Osm základních dimenzí je strukturováno podle dvou os. První osa postupuje od stavu nejniternějšího soukromí

---

[16] Viz WARREN, Samuel D., Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*, 1890, roč. IV, č. 5, s. 193–220.

[17] Viz WESTIN, Alan F. *Privacy and freedom*. New York: Atheneum, 1967.

[18] Viz CLARKE, Roger. Privacy Introduction and Definitions. *Roger Clarke's Web-Site*, publikováno 24. 6. 2016.

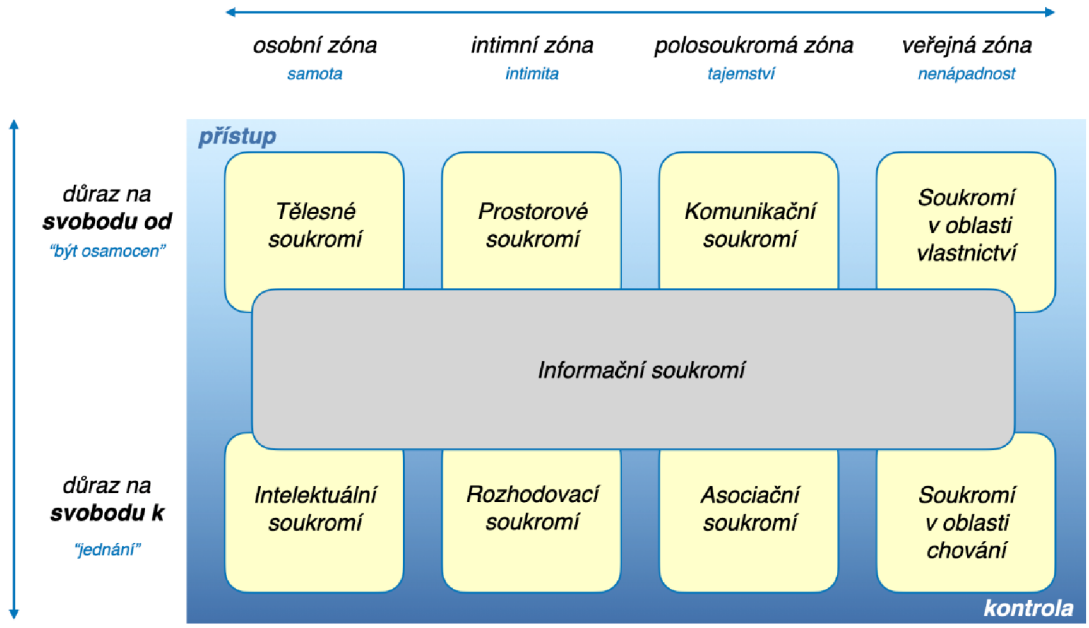
[19] Viz SOLOVE, Daniel J. Conceptualizing Privacy. *California Law Review*, 2002, roč. 90, č. 4, s. 1087–1155.

Dále SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 2006, roč. 154, č. 3, s. 477–564.

[20] Viz KOOPS, Bert-Jaap a kol. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 2017, roč. 38, č. 2, s. 483–576.

[21] Viz KOOPS, Bert-Jaap a kol. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 2017, roč. 38, č. 2, s. 506. Jde o tři státy angloamerické právní tradice (USA, Velká Británie a Kanada), tři státy kontinentální tradice spadající do oblasti západní Evropy (Nizozemí, Německo a Itálie) a tři státy kontinentální tradice spadající do oblasti střední a východní Evropy (Česká Republika, Polsko a Slovinsko).

(samoty), přes intimitu a tajemství, až po soukromí v rámci veřejného prostoru (nenápadnost).[22] Druhá osa pak odlišuje dvě polohy – akcent na ochranu daného práva (právo být nechán o samotě) a akcent na svobodu jednání. Onou devátou dimenzí soukromí je informační soukromí, které částečně překrývá osm zbývajících dimenzí.[23] Typologie je graficky znázorněna na Obr. 1.



Obr. 1: Typologie soukromí[24]

Informační soukromí představuje virtualizovanou[25] vrstvu ostatních dimenzí soukromí. Například otázka provedení tělesné prohlídky je v první řadě zásahem – v některých případech legitimním – do tělesného soukromí. Následně informace o výsledcích takové prohlídky však mohou zasahovat do soukromí informačního. Z hlediska použití technických prostředků pro zvládání pandemie můžeme již na základě předběžné úvahy předpokládat riziko zásahu takřka do všech uvedených dimenzí.[26] Hlavní tíhu však, zejména vzhledem k rozsáhlému zpracování dat, ponese informační soukromí jako

[22] V tomto směru navazuje na Westinovu typologii soukromí.

[23] Viz KOOPS, Bert-Jaap a kol. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 2017, roč. 38, č. 2, s. 566.

[24] Převzato z KOOPS, Bert-Jaap a kol. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 2017, roč. 38, č. 2, s. 566 a přeloženo.

[25] K virtualizaci obecně viz LÉVY, Pierre. *Becoming virtual: reality in the Digital Age*. New York: Plenum Trade, 1998.

[26] Snad s výhradou intelektuálního soukromí.

specifická dimenze zvolené typologie. Například fakt, zda je konkrétní osoba očkovaná nebo jaký je výsledek čerstvého testu, je otázkou tělesného soukromí. Šíření informací o těchto skutečnostech však bude spadat do dimenze soukromí informačního.[27]

Právo na soukromí je esenciálním právem, které je nezbytné pro zajištění autonomie jedince, výkon dalších jeho práv (svoboda projevu, svoboda náboženského vyznání) a jeho celkové fungování v demokratické společnosti.[28] Shodně se v tomto směru vyjadřuje i český Ústavní soud, který uvádí: *„Zcela zvláštní respekt a ochranu požívá v liberálních demokratických státech základní právo na nerušený soukromý život osoby (čl. 10 odst. 2 Listiny). Právo na nedotknutelnou soukromou sféru je úhelným kamenem liberální tradice, na které stojí základy moderní politiky i moderního práva, která rovněž stála u zrodu moderních idejí základních práv a svobod. Zajištění autonomní sféry jednotlivce je nejspolehlivější zárukou individuální nezávislosti a lidské svobody.“*[29] Na praktické úrovni je ochrana práva na soukromí nezbytná vzhledem k existenci tzv. chilling efektu. Tímto označením je popsán psychologický jev, kdy lidé, kteří ví, že jsou vystaveni neustálému sledování, upravují své jednání. Dochází u nich k automatickému přizpůsobení se požadované společenské normě a celkově se přestávají chovat skutečně svobodně.[30]

Koncept informačního soukromí je zejména v českém a německém prostředí úzce propojen s konceptem práva na informační sebeurčení. To bylo poprvé identifikováno německým Spolkovým ústavním soudem v roce 1983 v případě týkajícího se sčítání lidu.[31] Právo na informační sebeurčení spočívá v možnosti člověka stanovit si, zda a jakým způsobem mají být zveřejněny informace, které se ho týkají. Uvedené rozhodnutí

---

[27] Na tomto místě je třeba předeslat, že netvrdíme, že s těmito informacemi není možné pracovat. Jen je třeba mít na paměti rizika, která daná činnost představuje.

[28] Stejně viz WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.). *Právo na soukromí*. 1. vyd. Brno: Masarykova Univ., Mezinárodní Politologický Ústav, 2011, s. 53–54.

K tomu více viz REIMAN, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 1976, roč. 6, č. 1, s. 26–44.

[29] Viz bod 19 nálezu Ústavního soudu ze dne 2. 11. 2009, sp. zn. II. ÚS 2048/09, N 232/55 SbNU 181.

[30] Více k chilling efektu viz např. PENNEY, Jonathon. Chilling effects and transatlantic privacy. *European Law Journal*, 2019, roč. 25, č. 2, s. 122–139.

[31] Viz rozhodnutí německého Spolkového ústavního soudu ze dne 15. prosince 1983, sp. zn. BvR 209/83, BVerfGE 65.

německého Spolkového ústavního soudu pak zapůsobilo jako inspirace pro Ústavní soud, který koncept práva na informační sebeurčení převzal[32] a aplikoval jej v řadě svých rozhodnutí.[33]

Právo na soukromí je garantováno řadou mezinárodních dokumentů. Právo na ochranu soukromého života, rodiny, obydlí a korespondence je chráněno čl. 12 Všeobecné deklarace lidských práv z roku 1948 a čl. 17 Mezinárodního paktu o občanských a politických právech z roku 1966. Pro kontext pozitivněprávní úpravy je pak zásadní čl. 8 Evropské úmluvy o ochraně lidských práv (dále jen „EÚLP“), který garantuje právo na respektování rodinného a soukromého života. Samotný text čl. 8 obsahuje čtveřici garantovaných práv, konkrétně práva na respektování rodinného života, soukromého života, obydlí a konečně korespondence. Jak uvádí Evropský soud pro lidská práva (dále jen „ESLP“), jde o otevřené kategorie, protože právo na ochranu soukromého života nemá a ani nemůže mít vyčerpávající definici.[34] Ochrana práv zakotvených ve čl. 8 EÚLP tak v současné době zahrnuje i řadu dalších kategorií, které jsou z hlediska této výzkumné zprávy zásadní. Jde zejména o ochranu před odposlechy,[35] ochranu soukromí v kontextu

[32] Ústavní soud uvádí ve svých rozhodnutích jako základ práva na informační sebeurčení buď čl. 10 odst. 3 LZPS (viz bod 83 nálezu Ústavního soudu ze dne 12. 12. 2017, sp. zn. Pl. ÚS 26/16 a bod 301 nálezu Ústavního soudu ze dne 27. 11. 2012, sp. zn. Pl. ÚS 1/12, N 195/67 SbNU 333), nebo poměrně zajímavě kombinaci čl. 4 odst. 1 a čl. 2 odst. 2 (viz bod 27 nálezu Ústavního soudu ze dne 1. 12. 2008, sp. zn. I. ÚS 705/06, N 207/51 SbNU 577).

[33] V bodě 30 rozhodnutí Data retention I Ústavní soud uvádí: „*Pokud jednotlivci nebude garantována možnost hlídat a kontrolovat obsah i rozsah osobních dat a informací jím poskytnutých, jež mají být zveřejněny, uchovány či použity k jiným než původním účelům, nebude-li mít možnost rozpoznat a zhodnotit důvěryhodnost svého potenciálního komunikačního partnera a případně tomu uzpůsobit i své jednání, pak nutně dochází k omezení až potlačování jeho práv a svobod a nelze tak již nadále hovořit o svobodné a demokratické společnosti. Právo na informační sebeurčení (informationelle Selbstbestimmung) je tak nezbytnou podmínkou nejen pro svobodný rozvoj a seberealizaci jednotlivce ve společnosti, nýbrž i pro ustavení svobodného a demokratického komunikačního řádu. Zjednodušeně řečeno, v podmínkách vševědoucího a všudypřítomného státu a veřejné moci se svoboda projevu, právo na soukromí a právo svobodné volby chování a konání stávají prakticky neexistujícími a iluzorními.*“ Viz nález Ústavního soudu ze dne 22. 3. 2011, sp. zn. Pl. ÚS 24/10, N 52/60 SbNU 625. Mezi další významná rozhodnutí, ve kterých se Ústavní soud informačnímu sebeurčení věnoval, patří například nález Ústavního soudu ze dne 12. 12. 2017, sp. zn. Pl. ÚS 26/16 (nález ve věci EET), nález Ústavním soudu ze dne 21. 4. 2009, sp. zn. II. ÚS 703/06 a nález Ústavním soudu ze dne 17. 7. 2007, sp. zn. IV. ÚS 23/05, N 111/46 SbNU 41.

[34] Např. bod 33 rozsudku Evropského soudu pro lidská práva ze dne 4. 12. 2008 ve věci S. a Marper proti Spojenému království, stížnosti č. 30562/04 a 30566/04, nebo rozsudek ze dne 2. 8. 1984 ve věci Malone proti Spojenému království, stížnost č. 8691/79.

[35] Viz např. rozsudek Evropského soudu pro lidská práva ze dne 1. 7. 2008 ve věci Liberty a další proti Spojenému království, stížnost č. 58243/00, nebo rozsudek Evropského soudu pro lidská práva ze dne 4. 12. 2015 ve věci Roman Zakarov proti Rusku, stížnost č. 47143/06.

jednání na veřejnosti,[36] ochranu vlastního sebeurčení v souvislosti s ochranou osobní autonomie a možnosti osobního vývoje,[37] a ochranu zpracování osobních údajů obecně.[38] Na národní úrovni je pak v českém právním řádu ochrana soukromí zakotvena v Listině základních práv a svobod (dále jen „LZPS"), především v čl. 7 odst. 1, čl. 10 odst. 2 a 3 a čl. 13. Ústavní soud ve své praxi po vzoru ESLP přistupuje ke konceptu soukromého a rodinného života rovněž s tendencí k rozšiřování jeho výkladu.[39]

Právo na ochranu soukromého a rodinného života může být omezeno. To předpokládá ve svém textu EÚLP: *„Státní orgán nemůže do výkonu tohoto práva zasahovat kromě případů, kdy je to v souladu se zákonem a nezbytné v demokratické společnosti v zájmu národní bezpečnosti, veřejné bezpečnosti, hospodářského blahobytu země, ochrany pořádku a předcházení nepokojům a zločinnosti, ochrany zdraví nebo morálky nebo ochrany práv a svobod jiných."*[40] Omezení předpokládá také LZPS, která uvádí: *„Nedotknutelnost osoby a jejího soukromí je zaručena. Omezena může být jen v případech stanovených zákonem."*[41]

Podmínkou pro omezení práva na soukromý a rodinný život je, že (i) omezení musí být provedeno za jedním z účelů uvedených v čl. 8 odst. 2 EÚLP, (ii) musí být zakotveno v zákoně, a (iii) musí úspěšně projít testem proporcionality. V kontextu zásahu do soukromého a rodinného života se ve specifických případech mohou vyskytnout modifikované testy proporcionality.[42] Pro tuto výzkumnou zprávu nám však postačí

---

[36] Např. bod 57 rozsudku Evropského soudu pro lidská práva ze dne 25. 9. 2001 ve věci P.G. a J.H. proti Spojenému království, stížnost č. 44787/98, nebo body 58–59 rozsudku Evropského soudu pro lidská práva ze dne 28. 1. 2003 ve věci Peck proti Spojenému království, stížnost č. 44647/98.

[37] Uvedené dobře popsali Gellert a Gutwirth v jejich analýze rozhodnutí Evropského soudu pro lidská práva ve věcech Pretty proti Spojenému království (stížnost č. 2346/02), Evans proti Spojenému království (stížnost č. 6339/05) a Odièvre proti Francii (stížnost č. 42326/98). GELLERT, Raphaël, Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review*, 2013, roč. 29, č. 5, s. 524.

[38] Například rozhodnutí ve věcech Murray proti Spojenému království, stížnost č. 14310/88, Rotaru proti Rumunsku, stížnost č. 28341/95, Satakunnan Markkinapörssi Oy a Satamedia Oy proti Finsku, stížnost č. 931/13 a dalších.

[39] Viz např. nález Ústavního soudu ze dne 11. 11. 2005, sp. zn. I. ÚS 453/03, N 209/39 SbNU 215.

[40] Viz čl. 8 odst. 2 Evropské úmluvy o ochraně lidských práv.

[41] Viz čl. 7 odst. 1 Listiny základních práv a svobod.

[42] Např. test vyvážení ochrany soukromí a svobody projevu formulovaný v rozhodnutích Evropského soudu pro lidská práva ve věcech Von Hannover II (rozhodnutí Evropského soudu pro lidská práva ze dne 7. 2. 2012 ve věci Von Hannover proti Německu, stížnosti č. 40660/08 a 60641/08) a Axel Springer (rozhodnutí

klasický trojkrokový test proporcionality tvořený postupně kritériem vhodnosti, kritériem potřebnosti a samotným poměřováním kolidujících práv a zájmů. Řízení pandemie, tedy využívání technologických prostředků ke zvládání nákazy nebo k předcházení jejímu šíření, je bezpochyby oprávněným účelem, který je možné podřadit pod rozsah čl. 8 odst. 2 EÚLP. Konkrétně se jedná o účel zajištění veřejné bezpečnosti a ochrany zdraví. Nutnou podmínkou však zůstává řádné legislativní zakotvení.

Možnost omezit právo na ochranu soukromého a rodinného života však sama o sobě není bez limitu. Čl. 4 odst. 4 uvádí, že *„[p]ři používání ustanovení o mezích základních práv a svobod musí být šetřeno jejich podstaty a smyslu.“* Toto ustanovení, ve spojení s čl. 7 odst. 1 a čl. 10 LZPS, formulují jádro – samotnou podstatu – práva na ochranu soukromého a rodinného života. Toto jádro nemůže být omezeno a bude působit jako tvrdý limit pro nasazení specifických technických řešení. K povaze materiálního obsahu práva na soukromí Ústavní soud uvedl: *„Zachování materiálního obsahu práva na soukromí vyžaduje, aby v každém jednotlivém případě docházelo jen k takovému omezení základního práva, které je nutné a spravedlivě požadovatelné v demokratickém právním státě k tomu, aby byl ještě naplněn účel omezení. Jinými slovy, po identifikaci účelu, pro který má být základní právo omezováno, je třeba zkoumat, zda jde o omezení vhodné a potřebné (nutné) k tomu, aby byl dosažen aprobovaný cíl. Omezující zásah je vhodný, vykazuje-li takovou věcnou souvislost s účelem, že dosažení účelu přinejmenším podporuje. Potřebnost zásahu předpokládá, že k dispozici není žádný jiný, k právům dotčené osoby šetrnější, tj. menší újmu způsobující, a přitom stejně vhodný prostředek. Omezení základního práva na ochranu osobních údajů se nesmí vymykat z proporcionálního poměru k významu jím sledovaného cíle, […] tedy nesmí jít nad rámec toho, co je pro dosažení tohoto cíle nezbytné. Při splnění těchto předpokladů je omezení základního práva fyzické osoby jako individua vázaného na společenství a vztahujícího se k němu ospravedlnitelné.“*[43] Dále Ústavní soud jako samotnou podstatu práva na ochranu soukromí jednotlivce identifikoval požadavek *„respektu k svébytnému uspořádání života,*

Evropského soudu pro lidská práva ze dne 7.2. 2012 ve věci Axel Springer proti Německu, stížnost č. 39954/08).

[43] Viz bod 101 nálezu Ústavního soudu ze dne 20. 12. 2016, sp. zn. Pl. ÚS 3/14, 73/2017 Sb., N 246/83 SbNU 793.

jehož jednou z hlavních funkcí je zachování autonomie jednotlivce.“[44] Ve vztahu k tělesnému soukromí se k požadavku šetření podstaty a smyslu práva na ochranu soukromého a rodinného života Ústavní soud vyjádřil v otázce povinného očkování. Tam konstatoval, že pro zachování požadavků čl. 4 odst. 4 LZPS je nezbytné institut očkovací povinnosti doprovodit *„takovými zákonnými zárukami, jež by minimalizovaly jeho zneužití a vyloučily lékařský výkon v případě, že nejsou dány podmínky jeho provedení.“* [45]

Při pohledu do EÚLP je na první pohled očividné, že oproti národní úpravě neobsahuje garanci šetření podstaty a smyslu práv, které sama garantuje. Dle Wagnerové je tomu tak proto, že EÚLP je mezinárodněprávní nástroj, který primárně necílí na kontrolu a omezování zákonodárné moci v signatářských státech.[46] ESLP ale přesto pracuje s konceptem esence obsahu práv a nezbytností jejího zachování. Konkrétně k právům chráněným čl. 8 EÚLP soud uvádí, že tento článek chrání rovněž právo na osobní rozvoj, právo navazovat a rozvíjet vztahy s ostatními lidmi a s okolním světem. S člověkem by nemělo být zacházeno způsobem, který vede ke ztrátě jeho důstojnosti, neboť podstatou EÚLP je právě respekt k lidské důstojnosti a lidské svobodě.[47] Rozhodovací praxe ESLP zatím směřovala v kontextu vymezení esence čl. 8 EÚLP převážně k otázkám rodinného života než soukromí jako takového (viz např. Sheffield a Horsham proti Spojenému království[48] nebo Smith a Grady proti Spojenému království[49], přičemž oba případy se týkaly homosexuálních sňatků a svazků). V kontextu užití technologií (například ke sledování osob) prozatím ESLP k výslovnému vymezení esence čl. 8 nepřistoupil.[50]

---

[44] Viz bod 116 nálezu Ústavního soudu ze dne 3. 11. 2020, sp. zn. Pl. ÚS 10/17.

[45] Viz bod 71 nálezu Ústavního soudu ze dne 27. 1. 2015, sp. zn. Pl. ÚS 19/14, 97/2015 Sb., N 16/76 SbNU 231.

[46] Viz WAGNEROVÁ, Eliška. Čl.4 (Limity omezování základních práv). In: WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK, Ivo POSPÍŠIL aj. *Listina základních práv a svobod: Komentář* [Systém ASPI]. Wolters Kluwer, 2012.

[47] Viz bod 538 rozhodnutí Evropského soudu pro lidská práva ze dne 16. 2. 2015 ve věci Al-Nashiri proti Polsku, stížnost č. 28761/11.

[48] Viz rozsudek velkého senátu Evropského soudu pro lidská práva Sheffield a Horsham proti Spojenému království ze dne 30. 7. 1998, stížnosti č. 22985/93 a 23390/94.

[49] Viz rozsudek Evropského soudu pro lidská práva Smith a Grady proti Spojenému království ze dne 27. 8. 1999, stížnosti č. 33985/96 a 33986/96.

[50] Více viz BRKAN, Maja. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 2019, roč. 20, č. 6, s. 864–883.

Je také ještě nutné připomenout, že hledání podstaty základního práva představuje obtížný úkol. I přes výše uvedené snahy o abstraktní přístup k této otázce je nutné zdůraznit, že konečné hodnocení hranice základního práva je vždy podmíněno fakty situace, jejíž hodnocení je prováděno. Wagnerová k tomu uvádí, že *„podstatu základního práva [je] třeba hledat vždy v individuálním případě, neboť základní práva svědčí jednotlivcům. Pokud by se tedy podstata základního práva jevila zachovaná při posuzování omezení v abstraktní poloze, avšak v konkrétní věci by konkrétní osoba nebyla takovým základním právem vůbec chráněna, pak by jistě nebylo možno takové omezení, resp. vynulování základního práva tolerovat.“*[51] Tato výhrada souvisí se shora uvedenou metodologií a také s jedním z limitů této výzkumné zprávy. V závěru tak není možné nabídnout finální podobu nasazení technologických prostředků, které budou vždy použitelné právně souladným způsobem. Je ale možné zformulovat doporučení identifikující různá rizika nepřiměřeného zásahu do základního práva způsobeného konkrétním technickým nástrojem.

2.2. Ochrana osobních údajů

Právo na ochranu osobních údajů je doktrínou v dnešní době považováno za právo samostatné a na právu na soukromí nezávislé, ačkoli obě práva sledují v základu stejný cíl (ochranu soukromí jedince a následně nepřímo také ochranu dalších základních práv).[52] Od ochrany soukromí se však ochrana osobních údajů liší ve způsobech regulace. Ochranu osobních údajů můžeme chápat jako požadavek na korektní nakládání s informacemi,[53] díky čemuž působí jako nástroj prevence před zásahem do dalších práv a zájmů, které by mohly být nevhodným zpracováním poškozeny.[54] Ochrana osobních údajů je tedy do značné míry procedurální nástroj zajišťující vysokou úroveň ochrany práv a zájmů

[51] Viz WAGNEROVÁ, Eliška. Čl.4 (Limity omezování základních práv). In: WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK, Ivo POSPÍŠIL aj. *Listina základních práv a svobod: Komentář* [Systém ASPI]. Wolters Kluwer, 2012.

[52] Viz MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020, s. 47 a následující.

[53] Viz GELLERT, Raphaël, Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review*, 2013, roč. 29, č. 5, s. 525.

[54] Shodně viz HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/ 46/ EC and the General Data Protection Regulation. In: CREMONA, Marise (ed.). *New technologies and EU law*. First edition. New York: Oxford University Press, 2017, s. 123.

fyzických osob, kterých se osobní údaje týkají. Kromě toho je cílem právní úpravy v oblasti ochrany osobních údajů také umožnění korektního, férového a zákonného zpracování osobních údajů. V tomto se zmíněná úprava liší od právního rámce ochrany soukromí, který je od základu výhradně restriktivní a jeho omezení je podmíněno existencí zákonné výjimky a možností její aplikace na základě testu proporcionality v konkrétním případě. Ochrana osobních údajů však zpracování osobních údajů přímo předpokládá a stanovuje pravidla pro jeho provedení.[55]

Základním předpisem, který je v této oblasti nutné uvážit, je Obecné nařízení o ochraně osobních údajů (dále jen „GDPR“).[56] Do širšího rámce ochrany osobních údajů patří ještě směrnice č. 2016/680 upravující zpracování osobních údajů v kontextu prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, nařízení EU č. 1725/2018 upravující zpracování osobních údajů orgány Unie a zákon č. 110/2019 Sb., o zpracování osobních údajů. Tyto další předpisy však v problematice nasazování technologií za účelem zvládání pandemie nehrají vzhledem ke své působnosti podstatnou roli.

Pro potřeby této zprávy a zajištění širšího kontextu shrnujeme jen základní maxima právní úpravy ochrany osobních údajů. Ochrana osobních údajů se vztahuje na údaje, které mohou přímo či nepřímo vést k identifikaci fyzické osoby. Tu právní úprava označuje jako subjekt údajů. Čl. 4 odst. 1 GDPR pak uvádí, že osobní údaje jsou *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě […]; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“* Osobou zodpovědnou za zpracování je správce údajů, který určuje účel a prostředky zpracování

[55] Viz bod 4 odůvodnění GDPR, který stanoví, že *„Zpracování osobních údajů by mělo sloužit lidem. Právo na ochranu osobních údajů není právem absolutním; musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality musí být v rovnováze s dalšími základními právy.“*

[56] Jedná se o nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

osobních údajů a který plní další zákonné povinnosti, které zpracování vyžaduje.[57] Pro zahájení zpracování správce potřebuje disponovat jedním z právních titulů uvedených v čl. 6 odst. 1 GDPR. Zásadní roli pak při zpracování hraje zásada odpovědnosti správce, která se dále pojí s hodnocením rizik zpracování. Dle zásady odpovědnosti správce tento odpovídá za správnost prováděného zpracování a musí být schopný doložit, že osobní údaje zpracovává v souladu s GDPR (čl. 5 odst. 2 GDPR). V případě GDPR je možné setkat se s označením „regulace založená na riziku".[58] V praxi to znamená, že čím vyšší riziko dané zpracování osobních údajů pro práva a zájmy subjektu údajů představuje, tím pečlivěji a důkladněji musí být dané zpracování provedeno a dokumentováno.[59]

Správná aplikace pravidel ochrany osobních údajů je zcela nezbytná v průběhu nasazení technologických řešení, jejichž účelem je přispět ke zvládnutí pandemie, a při jejichž využívání dochází ke zpracování osobních údajů v jakékoli podobě. Dodržení zásad zpracování osobních údajů, ať už jde o základní principy formulované v čl. 5 odst. 1 GDPR nebo o konkrétní požadavky (např. zásada záměrné a standardní ochrany osobních údajů dle čl. 25 GDPR nebo zajištění zabezpečení zpracování dle čl. 32 GDPR) krom samotné legalizace zpracování výrazně snižuje rizika, která ze zpracování pro subjekty údajů vyplývají. V tomto ohledu není možné právní režim ochrany osobních údajů pominout. V této zprávě však není možné provést detailní hodnocení všech aspektů zpracování osobních údajů pro všechny případy nasazení technologií. Přímo to plyne z limitů zprávy, kdy hodnocení technologií provádíme v abstraktní rovině. Jde o podobný postup jako v případě hodnocení dopadů regulace na soukromí a zpracování osobních údajů, které je prováděno v rámci legislativního procesu.[60] Ani v tom případě nejsou hodnoceny konkrétní aplikace (resp. konkrétní parametry jejich nasazení), ale abstraktnější ústavně-právní limity připravovaných předpisů.

[57] Viz čl. 4 odst. 7 GDPR.

[58] Viz GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 2018, roč. 34, č. 2, s. 279–288.

[59] Více MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020, s. 159 a následující.

[60] Viz čl. 9 odst. 2 písm. h) Legislativních pravidel vlády ve znění novel.

Abstraktní zhodnocení vhodnosti a možností použití specifických technologií a identifikace jejich ústavních limitů je možné provést ruku v ruce s výše podaným výkladem práva na soukromí. Ochrana osobních údajů působí jako nástroj pro zajištění práva na soukromí, které je z hlediska vyhodnocení kolize s jinými právy a zájmy v takovém případě primární. Nenastane proto situace, kdy by kolize s jinými právy nebo zájmy (např. veřejným zájmem na zajištění veřejného zdraví při zvládání pandemie) byla prostřednictvím testu proporcionality vyhodnocena tak, že by nasazení technologie bylo z hlediska zásahu do práva na soukromí umožněno, ale zároveň by nebylo možné z hlediska práva na ochranu osobních údajů.[61] Vzhledem k tomu jsme se rozhodli dále se specificky ochraně osobních údajů ve zprávě nevěnovat a analýzu možnosti použití a dopadů vztahovat pouze k šířeji chápanému právu na ochranu soukromí, resp. právu na respektování soukromého a rodinného života ve smyslu čl. 8 EÚLP.

2.3. Dílčí závěr: Jádro práva na soukromí a role ochrany osobních údajů

Ze shora uvedeného plyne, že v kontextu práva na soukromí (respektive práva na rodinný a soukromý život) není možné jednoznačně definovat jeho nepřekonatelné jádro – esenci, která musí být vždy a za všech okolností zachována. To platí i přes to, že zejména české soudy s odkazem na čl. 4 odst. 4 LZPS s tímto konceptem operují. Naopak ESLP se v tomto směru doposud v oblastech relevantních pro tuto zprávu jednoznačně nevyjádřil. Na druhou stranu, zformulování hranice, kterou není v rámci hodnocení proporcionality překonat, protože by to znamenalo porušení čl. 4 odst. 4 LZPS, je pro naplnění cílů této zprávy nezbytné. Bez této hranice bychom totiž nemohli, ani na abstraktní úrovni, dojít k jakémukoli hmatatelnějšímu výsledku. Pro vymezení této hranice tak musíme vyjít z dostupných rozhodnutí Ústavního soudu a zejména z právní doktríny, která se věnuje právu na soukromí. Je třeba zdůraznit, že toto vymezení vytváříme v kontextu této zprávy. Nemáme tak ambice předkládat vymezení univerzálně platné.

Z výše citovaných zdrojů vyplývá, že jedním ze základních účelů práva na ochranu soukromí (respektive práva na soukromý a rodinný život) je zajištění svobody jedince. Za zcela neproporcionální, a proto nepřijatelné, tak musí být považováno takové použití

[61] Zdůrazňujeme, že toto je podmíněno skutečností, že správce údajů plní své povinnosti tak, jak z hlediska GDPR má.

technologie, které (i) povede k masovému plošnému nediskriminačnímu sledování obyvatel a které (ii) bude vzbuzovat chilling efekt způsobem, který povede k bránění ve výkonu dalších práv a svobod garantovaných LZPS.

Vzhledem k tomu, že při využívání technologických řešení pro zvládání pandemie bude v naprosté většině případů hrozit zejména zásah do oblasti informačního soukromí jedince, je dále možné vyjít z obecných zásad ochrany osobních údajů. Ty totiž s konceptem informačního soukromí velmi úzce souvisí a umožňují formulovat základní podmínky, které musí být vždy splněny. Ochrana osobních údajů jako regulatorní nástroj působí preventivně, a proto může vhodná aplikace těchto pravidel zajistit soulad využívaných technologií s ústavním pořádkem. Jde zejména o požadavky vyplývající z obecných zásad uvedených v čl. 5 GDPR, tedy o (i) zásadu zákonnosti, korektnosti a transparentnosti,[62] (ii) zásadu omezení účelem,[63] (iii) zásadu minimalizace údajů,[64] (iv) zásadu přesnosti,[65] (v) zásadu omezení uložení,[66] a (vi) zásadu integrity a důvěrnosti.[67]

Vedle uvedených zásad je pak nutné zdůraznit, že zpracování osobních údajů v kontextu nasazení technologických nástrojů pro zvládání pandemie bude většinově spadat do oblasti vysoce rizikového zpracování. Vzhledem k tomu je v souladu se zásadou odpovědnosti správce a s rolí hodnocení rizik při zpracování osobních údajů nezbytné, aby byly uvedené zásady plněny důkladně, korektně a precizně, a jejich plnění bylo náležitě dokumentováno. Jedná se o zcela nezbytnou podmínku, bez jejíhož dodržení nasazení technologického řešení nemůže právně obstát, byť by se jinak jádra práva na soukromý a rodinný život nedotýkalo.

---

[62] Zpracování osobních údajů musí probíhat na základě jasného zákonného zmocnění, transparentně a způsobem, který minimalizuje dopady na práva a zájmy subjektů údajů.

[63] Sesbírané osobní údaje nesmí být zpracovávané za jinými než předem deklarovanými účely.

[64] Zpracovány mohou být jen ty osobní údaje, které jsou striktně nezbytné pro dosažení požadovaného účelu.

[65] Zpracovávané osobní údaje musí být přesné. To je zejména zásadní v případě, že na základě tohoto zpracování dochází k rozhodování o právech a povinnostech subjektu údajů. V kontextu této výzkumné zprávy může jít například o vyhodnocování statusových certifikátů (očkování, testování) a na to navázané možnosti návštěv vybraných zařízení.

[66] Zpracovávané osobní údaje mohou být uloženy jen po dobu nezbytně nutnou pro naplnění daného účelu.

[67] Systém zpracování osobních údajů musí být nastaven tak, aby k údajům měly přístup jen osoby, které jej vzhledem k deklarovanému účelu zpracování mít musí. Zároveň musí být zabezpečen tak, aby se minimalizovalo riziko úniku osobních údajů.

3. Technologie používané ke zvládání pandemie covid-19

3.1. Přehled zemí s relevantním využitím technologií

3.1.1. Austrálie

V Austrálii byla v dubnu 2020 spuštěna a veřejnosti představena aplikace *COVIDSafe* určená pro vyhledávání kontaktů.[68] Využívání aplikace bylo zcela dobrovolné. Její tvůrci postupovali v souladu se zásadou záměrné ochrany soukromí (*privacy by design*).[69] Aplikace byla doprovázena přijetím zvláštní legislativy stanovující přísné sankce pro případ zneužití dat. Tato legislativa zároveň obsahovala ustanovení o ukončení její platnosti (*sunset clause*).[70] Pro spuštění aplikace se jedinec musel zaregistrovat. Zejména bylo nutné zadat údaje o jménu (přípustné bylo využití pseudonymu), věku (identifikací příslušného věkového rozsahu), telefonním čísle a poštovním směrovacím čísle. Aplikace využívala připojení Bluetooth, detekovala další zařízení s nainstalovanou aplikací *COVIDSafe* ve svém okolí a ukládala v zašifrované podobě údaje o kontaktu. Tyto údaje pak uchovávala po dobu 21 dní, po jejichž uplynutí došlo k automatickému smazání. K zašifrovaným údajům neměl uživatel aplikace přístup. V případě pozitivního testu uživatel aplikace nahrál data do systému *National COVIDSafe Data Store*, odkud mohli oprávněné osoby (pracovníci zdravotní správy) získat kontaktní údaje osob, u kterých došlo k blízkému kontaktu. Oficiální webová prezentace v závěru vybízela uživatele, aby po skončení pandemie aplikaci smazali. Provoz celého systému byl ukončen 16. 8. 2022. Kritická analýza ukázala, že aplikace nenaplnila očekávání, která do ní byla vkládána. Přínos pro zvládání pandemie byl ve srovnání s vynaloženými náklady zcela minimální.[71]

Dalším technologickým nástrojem používaným lokálně na území Nového Jižního Walesu byl sběr QR kódů identifikujících zákazníky ubytovacích zařízení. Sběr probíhal

[68] Pro další informace k aplikaci viz Australian Government Department of Health and Aged. COVIDSafe app. *Australian Government Department of Health and Aged Care*, publikováno 24. 4. 2020.

[69] Více k principu v CAVOUKIAN, Ann. *Privacy by Design - The 7 Foundational Principles*. IAPP, 2011, s. 1–9.

[70] Viz HENDRY, Justin. COVIDSafe privacy protections now locked in law. *iTnews*, publikováno 14. 5. 2020.

[71] Viz MOLLA, Alemayehu, Stan KARANASIOS. The COVIDSafe app is dead. What can we learn from this „failure"? *The Conversation*, publikováno 12. 8. 2022.

Viz VOGT, Florian a kol. Effectiveness evaluation of digital contact tracing for COVID-19 in New South Wales, Australia. *The Lancet Public Health*, 2022, roč. 7, č. 3, s. e250–e258.

prostřednictvím speciální aplikace provozované veřejným sektorem a jeho účelem bylo zajistit snadnější trasování kontaktů. Výhodou pro zapojené provozovatele ubytovacích zařízení bylo, že nemuseli řešit zpracování osobních údajů a jejich zabezpečení vlastními prostředky. Státní orgány pak mohly využít sesbírané údaje ke kontaktování osob v případě výskytu nákazy.[72] Nový Jižní Wales dále využil za účelem zjištění obecné úrovně dodržování epidemiologických opatření analýzu anonymizovaných provozních a lokalizačních údajů, které získal od telekomunikačních společností.[73] Nad těmito daty byla provedena analýza změn v mobilitě obyvatelstva v důsledku vyhlášených opatření omezujících svobodu pohybu.

Posledním významným technologickým řešením, které bylo v Austrálii využito, byly bezpilotní prostředky. S jejich pomocí byla kontrolována uzavřená hranice mezi státy Viktoria a Nový Jižní Wales.[74] Dalším využitím byla komunikace upozornění na porušení vyhlášených protiepidemických opatření a kontrola dodržování nařízeného společenského odstupu, kterou bezpilotními prostředky prováděly policejní složky Západní Austrálie.[75]

3.1.2. Brazílie

V Brazílii bylo využito několik technologických řešení pro vyhledávání a trasování rizikových kontaktů. První aplikace *Tô de Olho* byla vyvinuta a následně nasazena ve státě Rio Grande do Norte.[76] Skrze tuto aplikaci mohli její uživatelé ohlásit přítomnost velkého množství lidí na jednom místě. Aplikace uchovávala údaje o poloze zařízení, což umožňovalo trasování kontaktů a informování o riziku nákazy. Aplikace dále obsahovala mapy s vyznačením oblastí vysokého rizika nákazy a index izolovanosti jedinců v daných oblastech. Tvůrci aplikace veřejně přislíbili, že po skončení pandemie budou všechna

[72] Viz COVID-19 Update: NSW Businesses to use Service NSW QR Code. *Australian Institute of Food Safety,* publikováno 29. 12. 2020.

[73] Viz GRUBB, Ben. Mobile phone location data used to track Australians' movements during coronavirus crisis. *The Sydney Morning Herald*, publikováno 4. 4. 2020.

[74] Viz THORN, Adam. Drones to guard NSW-Vic border as Melbourne locks down. *Australian Aviation,* publikováno 7. 7. 2020.

[75] Viz WA police to use drones to enforce coronavirus restrictions. *9News*, publikováno 30. 3. 2020.

[76] Viz Aplicativo Tô de Olho ajuda a conter o coronavírus no RN. *Secretaria de Estado da Saúde Pública*, publikováno 8. 4. 2020.

shromážděná data smazána.[77] Za podobným účelem byla na federální úrovni nasazena aplikace *Coronavírus-SUS* vybudovaná na platformě *Apple/Google Exposure Notification*. Tato aplikace v případě pozitivního testu umožnila anonymně notifikovat další uživatele, kteří s pozitivně testovaným uživatelem přišli do blízkého kontaktu.[78] Aplikace dále sloužila jako informační nástroj pro obyvatelstvo. Obsahovala tak údaje a informace o symptomech a o prevenci, mapy umožňující najít blízké lékařské zařízení a také oficiální informace o nákaze, které vydávalo federální ministerstvo zdravotnictví.[79]

Brazilská vláda v dubnu 2020 přijala opatření, jímž nařídila telekomunikačním společnostem sdílet data (v rozsahu jména a adresy) s veřejnými institucemi za účelem provedení dálkových rozhovorů a sebrání údajů o ekonomických dopadech pandemie.[80] Toto opatření si vysloužilo značnou kritiku ze strany odborné veřejnosti i opozice. V červenci 2020 bylo toto kontroverzní nařízení Nejvyšším soudem zrušeno. Součástí rozhodnutí bylo i explicitní označení ochrany osobních údajů jako jednoho ze základních práv.[81]

Dalším technologickým nástrojem byla geolokalizační aplikace start-upu *InLoco*, která umožňovala hodnocení účinnosti opatření směřujících k omezení pohybu. Byla k tomu využita data z více než 60 milionů mobilních zařízení zapojených do služeb společnosti poskytujících geo-autentizaci a chránících proti podvodům.[82] *InLoco* vyvinula index sociální izolace, který umožňoval mapovat pohyb osob ve specifických oblastech. Aplikace pracovala s anonymizovanými agregovanými daty neumožňujícími přímou identifikaci

[77] Viz Aplicativo Tô de Olho ajuda a conter o coronavírus no RN. *Secretaria de Estado da Saúde Pública*, publikováno 8. 4. 2020.

[78] Viz MARI, Angelica. Brazil integrates Apple-Google exposure notification tech into coronavirus app. *ZDNet*, publikováno 5. 8. 2020.

[79] Viz Encontrar informações atualizadas sobre o coronavírus (Covid-19) — Português (Brasil). *gov.br*, citováno k 15. 7. 2022.

[80] Viz VIEIRA ALONSO, Fabio, Carolina BARBOSA DE L. CUNHA V DA COSTA. The impact of Covid-19 for data protection in Brazil: the perspective of Brazil's supreme court. *International Bar Association.*

[81] Viz SILVA, Ken. Brazilian court declares data protection a fundamental right in landmark decision. *Global Data Review,* publikováno 11. 5. 2020.

[82] Viz In Loco adapta sua tecnologia de geolocalização para ajudar no combate à Covid-19. *ABES*, publikováno 12. 4. 2020.

osob. Umožňovala také vládním orgánům reagovat v případě zjištění většího výskytu osob na jednom místě.[83]

Brazilské bezpečnostní složky ke kontrole dodržování omezujících opatření využívaly bezpilotní prostředky. Již v dubnu 2020 je implementovala například policie v Rio de Janeiro, která je využila jako informačního nástroje upozorňujícího na obsah vyhlášených omezujících opatření, a také k upozorňování občanů, kteří se účastnili zakázaných shromáždění. Drony byly opatřeny reproduktory a jejich prostřednictvím byli občané upozorňováni na nutnost zdržovat se ve svých domovech.[84]

3.1.3. ČLR

V Čínské lidové republice došly širokého využití zejména aplikace umožňující trasování osob. Příkladem je soubor aplikací souhrnně označovaných jako *Health Code*, které umožňovaly nejen trasování, ale sloužily také jako e-pas pro doložení aktuálního zdravotního stavu uživatele aplikace. Aplikace si jednotlivé správní celky tvořily samy, ale jejich cílová funkcionalita byla definována pokyny ústředních orgánů. Nadále k nim tedy přistupujeme pro jednoduchost jako k jednomu systému.[85] Uživatelé museli v aplikaci vyplnit údaje o historii svého pohybu, údaje o trvalém bydlišti a poskytnout relevantní zdravotní data. Obecně bylo používání aplikace povinné. Výjimku sice měli senioři, nicméně vzhledem k množství služeb, které byly na aplikaci (zejména na její funkci e-pasu) navázány, se aplikace stala faktickou nutností i pro ně.[86]

Aplikace na základě poskytnutých osobních údajů vytvořila pro uživatele QR kód, který komunikoval úroveň rizika spojenou s konkrétním uživatelem. Tato úroveň byla v aplikaci znázorněna barevným rozlišením ve třech stupních. Od nejrizikovější červené barvy přes středně rizikovou žlutou barvu až po bezrizikovou zelenou barvu. Uživatel, který byl

[83] Viz In Loco adapta sua tecnologia de geolocalização para ajudar no combate à Covid-19. *ABES*, publikováno 12. 4. 2020.

[84] Viz Río de Janeiro usa drones con altavoces para dispersar las aglomeraciones durante la pandemia. *La Vanguardia*, publikováno 15. 4. 2020.

[85] Viz SCHNEIDER, Florian, Rogier CREEMERS a kol. How Asia Confronts COVID-19 through Technology. *The Leiden Asia Centre,* 2021, s. 5–6.

[86] Viz WANG, Zhiqiong June, Jianfu CHEN. People's Republic of China: Legal Response to Covid 19. In: KING, Jeff, Octavio FERRAZ (eds.). *The Oxford Compendium of National Legal Responses to Covid-19*. Oxford University Press, 2021, odst. 84–86.

označen zeleným kódem nebyl ve svém pohybu nijak omezován. Osoby s dalšími stupni byly buď identifikovány jako osoby nakažené nebo osoby s vysokým rizikem nákazy. Pro tyto osoby byla nařízena izolace či byla jejich svoboda pohybu značně omezena. Schopnost jedince prezentovat se zeleným (bezrizikovým) QR kódem byla nezbytná pro využívání základních služeb jako např. městské hromadné dopravy, pro vstup do školských zařízení, restaurací, hotelů nebo obchodů s potravinami.[87] Požadované funkcionality měla aplikace *Health Code* samostatně nebo byly tyto funkcionality integrovány do již existujících a široce rozšířených aplikací. Jako příklad je možné uvést komunikační a sociální aplikaci *WeChat* nebo platební aplikaci *Alipay*.[88] V dalších verzích *Health Code* pak bylo možné i kontrolovat, zda uživatel dodržuje nařízená karanténní či izolační opatření. Data byla v tomto kontextu používána pro automatizovanou kontrolu pohybu a pobytu uživatelů aplikace. Z dostupných článků v médiích plyne podezření, že aplikace zpracovávala osobní údaje ve větší než deklarované míře, a tato data bez vědomí a souhlasu uživatelů sdílela s policejními složkami.[89]

Také v ČLR došlo k využití bezpilotních prostředků. Drony sloužily jako nástroj pro kontrolu dodržování zavedených opatření.[90] Některé typy dronů využívané v zemědělství byly použity k dezinfekci míst s větší koncentrací osob.[91] Bezpilotní prostředky také v některých oblastech doručovaly potraviny a léky pro osoby s nařízenou izolací.[92]

---

[87] Viz LIANG, Fan. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. *Social Media + Society*, 2020, roč. 6, č. 3, s. 1–4.

[88] Viz SCHNEIDER, Florian, Rogier CREEMERS a kol. How Asia Confronts COVID-19 through Technology. *The Leiden Asia Centre,* 2021, s. 5–6.

[89] Viz TANGERMANN, Victor. In China, this coronavirus app pretty much controls your life. *Futurism,* publikováno 16. 4. 2020.

[90] Viz BURKI, Talha. China's successful control of COVID-19. *The Lancet Infectious Diseases*, 2020, roč. 20, č. 11, s. 1240.

[91] Viz SOO LINDBERG, Kari, Colum MURPHY. Drones Take to China's Skies to Fight Coronavirus Outbreak - Bloomberg. *Bloomberg*, publikováno 4. 2. 2020.

Také YANG, Junwei, Timothy REUTER. 3 ways China is using drones to fight coronavirus. *World Economic Forum,* publikováno 16. 3. 2020.

[92] Viz YANG, Junwei, Timothy REUTER. 3 ways China is using drones to fight coronavirus. *World Economic Forum,* publikováno 16. 3. 2020.

Také 10 Ways Technology is Helping To Fight the Coronavirus. *UNDP*, publikováno 27. 2. 2020.

Na některých místech byly nasazeny dálkové teploměry, které měly za cíl vytipovat osoby s vyšší tělesnou teplotou (jeden z příznaků probíhající infekce včetně infekce koronavirem SARS-CoV-2. Tyto teploměry byly umisťovány v prostředcích městské hromadné dopravy a byly propojeny s technologií rozpoznávání obličejů.[93]

3.1.4. EU

Stejně jako v ostatních státech bylo i na území EU využito mobilních aplikací. EU v tomto kontextu spustila *European Federation Gateway Service*. V rámci přípravy této iniciativy byla přijata sada opatření, která měla zajistit jednotný společný postup v oblasti interoperability, technických specifikací a architektury. Pro zařazení do této iniciativy musela konkrétní aplikace splňovat standardy v oblasti ochrany osobních údajů a zabezpečení dat. Dále musela aplikace upřednostňovat decentralizované využití technologie Bluetooth před využitím centralizovaných systémů nebo lokalizačních údajů. Aplikace byly dominantně postaveny na technologii *Apple/Google Exposure Notification*. Jednalo se například o německou *Corona-Warn-App* nebo italskou *Immuni*. Výjimkou pak byly například aplikace *Virus Radar* (Maďarsko) nebo *TousAntiCovid* (Francie), které nebyly s celounijním systémem trasování kompatibilní.[94]

European Federation Gateway Service byla následně využita také pro ověřování certifikátů o očkování, testování nebo prodělání nemoci covid-19. *EU Digital COVID Certificate* obsahoval QR kód s digitálním podpisem vydavatele certifikátu (např. zdravotnické zařízení, které provedlo očkování nebo testování). Údaje, především digitální podpisy, byly centralizovaně ukládány v národní databázi a jejich vzájemné ověřování probíhalo skrze bránu Evropské unie.[95]

V některých zemích EU došlo k využití bezpilotních prostředků. Ve Španělsku či Francii byly drony využity pro kontrolu dodržování omezujících opatření.[96] Ve městě Burgas

[93] Viz GUZMAN, Joseph. China rolls out facial recognition thermometers on buses amid coronavirus outbreak. *TheHill*, publikováno 19. 2. 2020.

[94] Viz How tracing and warning apps can help during the pandemic. *European Commission*. Také Coronavirus: EU interoperability gateway for contact tracing and warning apps – Questions and Answers. *European Commission*, publikováno 19. 10. 2020.

[95] Viz EU Digital COVID Certificate. *European Commission*.

[96] Viz DIMITROVA, Aseniya. How drones help cities during the Covid-19 pandemic. *TheMayor.EU*, publikováno 23. 3. 2020.

v Bulharsku pak byly na drony připevněny teploměry pro dálkové měření teploty občanů. Opatření bylo předmětem velmi silné kritiky, neboť bezpilotní prostředky byly využívány primárně v částech města osídlených tamní romskou komunitou.[97]

3.1.5. Japonsko

Také v Japonsku byla nasazena aplikace k usnadnění trasování a k vyhodnocování epidemiologicky relevantních kontaktů. Aplikace *COCOA* (*COVID-19 Contract-Confirming Application*) využívala technologii Bluetooth. Data o blízkosti dvou telefonů uchovávala po dobu 14 dní a následně je automaticky mazala. Aplikace byla v Japonsku nasazena v červnu 2020 v rámci tamní první vlny šíření onemocnění covid-19.[98]

Silnou úlohu hrála v Japonsku aplikace pro osoby přijíždějící do země. Aplikace *OEL* (*Overseas Entrants Locator*) zejména sledovala dodržování povinné 14denní karantény po příjezdu do země. Tato aplikace nesledovala uživatele skrze jejich polohu kontinuálně. Kontroly osob prostřednictvím této aplikace probíhaly tak, že se uživatelům pravidelně zobrazovala notifikace. Reakcí na tuto notifikaci došlo k odeslání polohy uživatele a tím k ověření, zda uživatel nařízenou karanténu opravdu dodržuje. Pokud uživatel mobilního zařízení na notifikaci nereagoval, byl následně zkontrolován prostřednictvím telefonátu, Skype nebo e-mailu od japonských úředníků. Pro fungování aplikace byl nezbytný chytrý telefon a stát za tímto účelem zapůjčoval chytré telefony osobám, které do země přicestovaly bez nich.[99]

Od konce roku 2021 byla v Japonsku uvedena do provozu aplikace *COVID-19 Vaccination Certificate Application* obsahující certifikát o očkování. Prezentace certifikátu v aplikaci byla předpokladem ke vstupu jedinců na veřejné akce (např. koncetry) a do vybraných typů zařízení (např. restaurace). Zároveň byla tato aplikace napojena na národní identifikační systém.[100]

---

[97] Viz RYŠAVÝ, Zdeněk. Amnesty International tvrdě kritizuje uzavírání romských osad na Slovensku a v Bulharsku. *Romea.cz*, publikováno 20. 4. 2020.

[98] Viz Japan's COVID-19 app failed to pass on some contact warnings. *Reuters*, publikováno 3. 2. 2021.

[99] Viz OSUMI, Magdalena. How Japan tracks arrivals from abroad to curb the spread of new virus strains. *The Japan Times*, publikováno 29. 3. 2021.

[100] Viz Japan launches COVID vaccine certificate app. *Nikkei Asia*, publikováno 20. 12. 2021.

3.1.6. JAR

Jihoafrická republika také využívala technologické nástroje pro zmírnění pandemie. V březnu 2020 se vláda dohodla s jihoafrickými telekomunikačními společnostmi na poskytování analytických služeb na základě dat o poloze mobilních telefonů. Data byla využívána v rámci aplikace *COVID-19 Tracing Database*, jejíž funkcí bylo trasování kontaktů nakažených osob. Aplikace pracovala s osobními údaji sledovaných osob (jméno, číslo pasu, adresa trvalého pobytu, informace o pozitivních testech). Zahrnovala také údaje o pobytu a pohybu osob s pozitivním testem nebo sbírala informace o jejich kontaktech. Zajímavé je, že aplikace fungovala nezávisle na souhlasu sledovaných osob.[101] Data byla do *COVID-19 Tracing Database* ukládána od března 2020 do počátku dubna 2022. Po tomto datu mělo dojít v horizontu šesti týdnů k informování všech osob, jejichž údaje byly do databáze zahrnuty, podle dostupných informací k tomu však dosud nedošlo.[102]

Na místní úrovni docházelo v JAR k využívání bezpilotních prostředků. Ty byly nasazovány zejména za účelem edukace osob v odlehlých venkovských oblastech. Právě široká informovanost o nemoci a jejím průběhu měla zabránit přetížení nemocnic.[103]

Využití se dočkaly také některé rozšířené komunikační platformy, např. *WhatsApp*. Tato aplikace byla v některých provinciích JAR využita jako prostředek pro trasování kontaktů a ke sdílení výsledků testů.[104] Oficiální trasovací aplikace, *COVID Alert SA*, pak využívala technologii Bluetooth prostřednictvím *Apple/Google Exposure Notification*. Použití aplikace bylo dobrovolné, aplikace nebyla propojena s národní databází ani nevyužívala údaje o poloze zařízení. Vědci byl popsán pozitivní vliv aplikace na omezení šíření onemocnění.[105]

---

[101] Viz The end of South Africa's state of disaster and lockdown restrictions is coming. *BusinessTech,* publikováno 10. 12. 2021.

[102] Viz BODA, Ridwaan. South Africa: Contact tracing and its aftermath. *DataGuidance*, publikováno 8. 9. 2022.

[103] Viz KLERK, Marize de. Drones Spread Word About COVID-19 in Rural South Africa. *VOA*, publikováno 28. 4. 2020.

[104] Viz FULL SPEECH: Ramaphosa's address to the nation. *Eyewitness news,* publikováno 12. 7. 2020

[105] Viz KINYILI, Musyoka, Justin B. MUNYAKAZI, Abdulaziz YA MUKHTAR. Mathematical modeling and impact analysis of the use of COVID Alert SA app. *AIMS Public Health*, 2021, roč. 9, č. 1, s. 124–125.

3.1.7. Korejská republika

Korejská republika představuje ve srovnání s ostatními zeměmi specifický případ. Vzhledem ke značné technologické vyspělosti země i jejích obyvatel byly technologie používány výrazně více než v jiných zemích.[106] Ústředním pilířem korejské strategie bylo trasování. To probíhalo za intenzivní spolupráce mezi veřejným a soukromým sektorem. Došlo k využití GNSS údajů o poloze a pohybu osob, údajů o karetních transakcích či záznamů z veřejných kamer. Masivní využití těchto technologií bylo možné především díky solidnímu právnímu zázemí. Spolu s trasováním byla využita média (televizní a rozhlasové vysílání), kde odcházelo ke zveřejňování údajů o pobytu nakažených osob.[107] Se sdílením dat o poloze nakažených se pojilo velké množství iniciativ soukromého sektoru.[108] Konkrétním příkladem může být aplikace *Corona 100m*, která uživatele informovala o tom, že se pohybuje v okruhu 100m od místa, kde se nachází nebo nacházela infikovaná osoba. Na podobném principu byla založena i aplikace *Corona Map*, která také upozorňovala na místa s výskytem infikovaných osob.[109]

Další kategorie použitých technologií je spojována s izolací a karanténou jednotlivých osob. S pomocí aplikace *Smart Quarantine System* bylo možné monitorovat osoby, které vstoupily na území země.[110] Tento systém byl podobný japonské aplikaci *OEL*. Další aplikací využívanou v kontextu nařizování a sledování karantény byla *Self-quarantine Safety Application*. Tato aplikace sloužila dvojímu účelu. Primárně se jednalo o nástroj, který pomocí GNSS lokalizoval osobu a kontroloval dodržování nařízené karantény. Následně

[106] Viz CHUNG, Sunghee, Sujin LEE. South Korea: Democracy, Innovation, and Surveillance. In: RAMRAJ, Victor Vridar (ed.). *COVID-19 in Asia: law and policy contexts*. New York: Oxford University Press, 2021, s. 242.

[107] Viz CHUNG, Sunghee, Sujin LEE. South Korea: Democracy, Innovation, and Surveillance. In: RAMRAJ, Victor Vridar (ed.). *COVID-19 in Asia: law and policy contexts*. New York: Oxford University Press, 2021, s. 242–243.

[108] Dále HUANG, Yasheng, Meicen SUN a Yuze SUI. How Digital Contact Tracing Slowed Covid-19 in East Asia. *Harvard Business Review*, publikováno 15. 4. 2020.

[109] Viz CHUNG, Sunghee, Sujin LEE. South Korea: Democracy, Innovation, and Surveillance. In: RAMRAJ, Victor Vridar (ed.). *COVID-19 in Asia: law and policy contexts*. New York: Oxford University Press, 2021, s. 247.

[110] Viz HEO, Kyungmoo, Daejoong LEE, Yongseok SEO a kol. Searching for Digital Technologies in Containment and Mitigation Strategies: Experience from South Korea COVID-19. *Annals of Global Health*, 2020, roč. 86, č. 1, art. 109.

aplikace sloužila pro samodiagnostiku a také k šíření informací o onemocnění covid-19.[111] Samostatnou kategorií pak byla rozsáhlá nabídka aplikací čistě informativního charakteru. Ty informovaly o nejbližším testovacím místu, přijatých opatřeních nebo uživatele navedly k nejbližšímu místu se zásobou roušek.[112]

Korejská republika se pokusila o implementaci invazivnějších technologických nástrojů. Konkrétně se jednalo o zavedení elektronických náramků pro sledování pohybu a pobytu osob v karanténě. Původně mělo být nošení těchto náramků povinné pro všechny osoby, které porušily nařízenou karanténu, a to i bez jejich souhlasu.[113] Nakonec bylo opatření zmírněno a pro aplikaci náramku byl nezbytný souhlas.[114]

3.1.8. Ruská federace

Prvním technickým opatřením, které Ruská federace v dubnu 2020 zavedla, byl systém vycházkových propustek skrze SMS zprávy. Ty museli posílat obyvatelé vybraných oblastí (nejednalo se o opatření platné na federální úrovni), kteří chtěli opustit bydliště. Data o udělených propustkách se shromažďovala a vyhodnocovala v centrálním úložišti. Řešení mělo představovat alternativu ke sledovacím aplikacím pro obyvatele bez chytrých telefonů. Ukázalo se však, že opatření nepřináší plánované výsledky, a tak bylo po několika týdnech zrušeno. Například v Moskvě se však podobný systém digitálních propustek udržel a s drobnými úpravami pokračoval i dále. Propustky byly aktivně kontrolovány při využívání hromadné dopravy či policejními složkami.[115]

---

[111] Viz CHUNG, Sunghee, Sujin LEE. South Korea: Democracy, Innovation, and Surveillance. In: RAMRAJ, Victor Vridar (ed.). *COVID-19 in Asia: law and policy contexts*. New York: Oxford University Press, 2021, s. 244–245.

[112] Viz How Korean mobile apps are making COVID-19 resources more accessible. *GoodUX*.

[113] Viz Korea to use electronic bracelets on violators of self-isolation rules. *koreatimes*, publikováno 11. 4. 2020.

[114] Viz CHUNG, Sunghee, Sujin LEE. South Korea: Democracy, Innovation, and Surveillance. In: RAMRAJ, Victor Vridar (ed.). *COVID-19 in Asia: law and policy contexts*. New York: Oxford University Press, 2021, s. 245.

[115] Viz COVID-19 Health System Response Monitor (HSRM): Russian Federation. *European Observatory on Health Systems and Policies*.

Dále MAKARYCHEV, Andrey, Maria GOES, Anna KUZNETSOVA. The Covid Biopolitics in Russia: Putin's Sovereignty versus Regional Governmentality. *Czech Journal of International Relations*, 2020, roč. 55, č. 4, s. 38–39.

Vedle výše popsaného nástroje byly v Rusku využívány i sledovací aplikace. Příkladem byla *StopCoronaVirus My Contacts*, která byla vydána a provozována Ministerstvem pro digitální rozvoj, komunikaci a masová média. Aplikace měla za cíl trasování kontaktů a využívala především technologii Bluetooth. Aplikace fungovala na základě dobrovolného hlášení pozitivních testů uživateli. Na základě vložení záznamu o pozitivním testu došlo k identifikaci rizikových kontaktů a jejich následnému oslovení.[116]

Kromě této oficiální aplikace existovaly i další nástroje. Jedním z nich byla aplikace používaná v Moskvě, která sloužila zejména jako nástroj pro kontrolu dodržování karanténních opatření. Osoby, které karantény porušily, byly na základě informací z aplikace sankcionovány.[117] Později však bylo zjištěno, že na základě chyby v aplikaci dochází k uložení sankcí i osobám, které nařízenou karanténu neporušily.[118] Tato aplikace pro své použití vynucovala přístup k poloze zařízení, informaci o síti, záznamu telefonátů, kameře i dalším datům. Vzhledem k absenci odůvodnění přístupu ke všem těmto datům panovaly ohledně používání aplikace obavy.[119]

Kamerový systém *Bezpečné město* byl od února 2020 nasazen pro kontrolu nařízených izolací. Systém byl propojen s technologií na rozpoznávání obličejů a propojen s projektem digitálních propustek. Podle zpráv měl odhalit více než 200 osob porušujících nařízenou karanténu.[120]

---

[116] Viz GERDO, Vladimir. Russia Develops Coronavirus Contact-Tracing App. *The Moscow Times*, publikováno 17. 11. 2020.

[117] Viz MAYNES, Charles. Moscow To Launch New Surveillance App To Track Residents In Coronavirus Lockdown. *NPR*, publikováno 1. 4. 2020.

[118] Viz Russia: Intrusive Tracking App Wrongly Fines Muscovites. *Human Rights Watch*, publikováno 21. 5. 2020.

[119] Viz STEVENS, Robert. Russia's coronavirus app is turning it into a police state. *Decrypt*, publikováno 2. 4. 2020.

[120] Systém byl spuštěn v roce 2019 a zahrnoval asi 180 tisíc kamer. Viz WOODHAMS, Samuel. COVID-19 Digital Rights Tracker. *TOP10VPN*, publikováno 20. 3. 2020.

Dále Kamery videonabljuděnija v Moskvě vyjavili boljeje 200 graždan, narušivšich režim samoizoljacii [orig. Камеры видеонаблюдения в Москве выявили более 200 граждан, нарушивших режим самоизоляции]. *TASS* [orig. ТАСС], publikováno 18. 3. 2020.

Také Russia uses facial recognition to tackle virus. *BBC News*, publikováno 4. 4. 2020.

3.1.9. Velká Británie

Příkladem využití technologií ve Velké Británii byla aplikace *COVID Symptom Study.* Tento nástroj byl vyvinut soukromou zdravotnickou společností za podpory úřadů Walesu a Skotska. Uživatelé mohli v rámci aplikace zaznamenávat příznaky své i svých blízkých. Na základě získaných dat pak byly modelovány algoritmy predikující počty nakažených a usnadňující sledování rozvoje onemocnění. Zároveň byla tato aplikace využita jako podkladový zdroj pro studii o proměnách symptomů na základě osobních charakteristik.[121]

Ve Velké Británii došlo k využití bezpilotních letounů. Britská policie jich využívala pro sledování dodržování omezujících opatření. Kromě toho policejní složky aktivně využívaly pro sledování pohybu osob systémy na rozpoznávání registračních značek automobilů.[122]

V místech s větší koncentrací osob (letiště Heathrow, přístav Portsmouth, prostory společnosti Amazon) byly testovány či přímo do provozu zavedeny kamerové systémy snímající teplotu lidského těla. Tyto systémy zpracovávaly a ukládaly množství osobních údajů (pohlaví, věk). Některé instituce zvažovaly propojení těchto teploměrů se systémy pro rozpoznávání obličejů. Tento postup byl ale v kontextu malé efektivity nástroje (zvýšená tělesná teplota není spolehlivým indikátorem onemocnění covid-19) a velkého zásahu do soukromí značně kritizován.[123]

Existující sledovací technologie, jako jsou městské kamerové systémy, pak byly používány pro kontrolu dodržování rozestupů nebo kontrolu dodržování omezujících opatření

[121] Viz About the ZOE COVID Study. *ZOE COVID Study*.

[122] Jednalo se o kontroverzní technologii *Automated Number Plate Recognition*.

Viz BIENKOV, Adam. UK police officers are using drones to „lockdown shame" people for walking their dogs in remote areas during the coronavirus outbreak. *Business Insider*, publikováno 27. 3. 2020.

Viz iNews — Police Filming Innocent Members of the Public With Drones and Putting It Online. *Big Brother Watch*, publikováno 27. 3. 2020.

Dále viz LANGFORD, Eleanor. Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns. *Politics Home*, publikováno 17. 9. 2020.

[123] Viz *Emergency Powers and Civil Liberties Report – May 2020*. Big Brother Watch, 2020, s. 86–95.

Dále *Emergency Powers and Civil Liberties Report – June 2020*. Big Brother Watch, 2020, s. 64–66.

Také viz *Emergency Powers and Civil Liberties Report – October 2020*. Big Brother Watch, 2020, s. 40–44.

(povolené individuální procházky apod.) např. v Londýně,[124] Oxfordu, Manchesteru, Cambridge nebo Nottinghamu.[125]

Aplikace *NHS Test and Trace* měla být spuštěna v květnu 2020. Její první nasazení však bylo odloženo za účelem její úpravy pro využití *Apple/Google Exposure Notification*. Oficiálně tak byla spuštěna až v září 2020. Kromě upozornění na riziko kontaktu s infikovanou osobou fungovala aplikace také jako zdroj informací. S aplikací bylo spojeno i využívání QR kódů použitelných při trasování. Provozovatelé některých služeb (restaurace, bary, kadeřnictví apod.) měli povinnost vystavit QR kód u vstupu do provozovny. Návštěvníci pak tento kód museli aplikací naskenovat. Na základě toho pak byly vytvářeny seznamy potenciálně rizikových kontaktů, které byly využívány v případě zachycení pozitivního případu.[126] Podobnou funkci plnila aplikace *Protect Scotland* využívaná ve Skotsku, velšská *NHS Covid-19* nebo severoirská *StopCOVID NI.*[127]

3.2. Typologie technologií podle účelu nasazení

3.2.1. Trasování kontaktů

Základním a zdaleka nejpoužívanějším technologickým řešením byly prostředky usnadňující trasování epidemiologicky významných kontaktů. Tento cíl byl naplňován několika různými způsoby, které se liší technickou a ekonomickou náročností, ale i svými právními dopady.[128] Tyto nástroje měly umožnit zmapování rozsahu nákazy a přispět k lokalizaci jejího šíření. To následně mělo přispět ke zpomalení průběhu pandemie včasnou izolací osob, které byly v blízkém kontaktu s nakaženým jedincem. Funkční trasování kontaktů je vhodným prostředkem pro zamezení nutnosti plošně omezovat

[124] Viz ROACH, April. AI cameras being used on UK streets to monitor social distancing. *Evening Standard,* publikováno 8. 10. 2020.

[125] Viz TINGLE, Rory. 1,000 AI scanners are monitoring how close pedestrians are walking. *Mail Online,* publikováno 9. 10. 2020.

[126] Viz Which venues in England should display the official NHS QR code poster? *NHS*, citováno k 13. 6. 2022. Také viz *Emergency Powers and Civil Liberties Report – June 2020*. Big Brother Watch, 2020, s. 43–49.

[127] Viz MEDINA-PEREA, Itzelle A. Do contact-tracing apps have a future? *The Conversation*, publikováno 16. 3. 2022.

[128] Dobrý přehledový text nabízí HOGAN, Katie, Briana MACEDO, Venkata MACHA, Arko BARMAN, Xiaoqian JIANG. Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation. *JMIR Medical Informatics*, 2021, roč. 9, č. 7, e27449.

svobodu pohybu. Virtualizuje totiž hlavní důvod, pro který se omezení svobody pohybu zavádí, a to omezení rizikových kontaktů a snížení rizika šíření agens.

Identifikovali jsme čtyři následující varianty tohoto způsobu využití technologie.

Nástroje využívající protokol Bluetooth pro detekci zařízení s nainstalovanou aplikací v blízkém okolí. Varianta využívá protokolu Bluetooth. Prostřednictvím něj spolu mohou na krátkou vzdálenost komunikovat mobilní zařízení, která mají nainstalovanou a spuštěnou stejnou (nebo kompatibilní) aplikaci. Na základě blízkosti je pak uveden záznam o kontaktu. V případě potvrzení nákazy u konkrétního jedince jsou kontakty nakažené osoby upozorněny a je jim doporučeno (nebo nařízeno) omezení kontaktů či otestování. Rozšířeným technickým řešením této varianty je platforma *Apple/Google Exposure Notification*.

Výhodou této varianty (tedy využití protokolu Bluetooth) je efektivní využití principu záměrné ochrany osobních údajů (*data protection by design*), kdy nejsou vůbec zpracovávána geografická data o pohybu zařízení, ale kontakty jsou vyhodnocovány pouze vůči sobě. Silná pseudonymizace a technické zabezpečení pak zajistí, že uživatelé aplikace nedokáží zjistit, s jakými zařízeními (a jejich uživateli) se setkali. Silnou nevýhodou této varianty trasování je, krom nákladů spojených s jejím vývojem a implementací, nezbytnost rozšířit aplikaci mezi významnou část obyvatelstva. Značným limitem, zejména v některých regionech, také je, že všichni uživatelé musí vlastnit kompatibilní chytré mobilní zařízení.

Tato varianta trasování kontaktů patřila mezi silně rozšířené. K jejímu využití došlo v Austrálii (*COVIDSafe*), Brazílii (*Coronavírus-SUS*), ČLR (*Health Code*), Německu (*Corona-Warn-App*), Itálii (*Immuni*), Japonsku (*COCOA*), JAR (*COVID Alert SA*), Ruské federací (*StopCoronaVirus My Contacts*) nebo Velké Británii (*NHS Test and Trace*). Krom uvedených příkladů je možné zmínit, že do této kategorie spadá i aplikace *eRouška* využívaná v ČR. Alternativou k mobilní aplikaci, která však byla postavená na stejném principu, byly Bluetooth náramky používané v přístavu v Antverpách, které zajišťovaly trasování osob pohybujících se v přístavu.[129]

[129] Viz *Digital Solutions to Fight Covid-19. 2020 Data Protection Report*. Council of Europe, 2020, s. 20.

Zaznamenávání pohybu zařízení v prostoru prostřednictvím mobilní aplikace a GNSS. Tato varianta trasování spočívá v zaznamenávání polohy a pohybu mobilního zařízení, k čemuž je využívána v něm nainstalovaná aplikace. V případě potvrzení nákazy uživatele jsou upozorněny osoby, které se v průběhu relevantního časového úseku nacházely v jeho blízkosti. Na rozdíl od předchozí varianty trasování se blízkost nehodnotí relativně na základě kontaktu zařízení, ale absolutně vzhledem ke geografické poloze.

Zřejmou nevýhodou této varianty trasování je větší množství zpracovávaných osobních údajů, což může vést k porušení zásady minimalizace údajů. Je také velmi obtížně vyhodnocovat kontakty uvnitř budov nebo v místech s horším pokrytím družicovým signálem. Výhodou je naopak následná možnost tato data využívat pro analýzu hotspotů s velkým výskytem osob a tím větším rizikem nákazy.

Tato varianta trasování byla využita například v Brazílii (*Tô de Olho*) a Korejské republice (*Corona 100m a Corona Map*). V českém kontextu byl obdobný nástroj krátce přítomný jako modul v aplikaci *Mapy.cz.*[130]

Zaznamenávání pohybu zařízení v prostoru s využitím provozních a lokalizačních údajů. Tato varianta vychází z možnosti spolupráce státu s poskytovateli služeb elektronických komunikací (respektive z možnosti státu nařídit těmto poskytovatelům předávat provozní a lokalizační údaje o klientech státním organizacím). Tato varianta se z hlediska technického provedení poměrně silně nabízí, protože se jedná o data, která poskytovatelé elektronických komunikací typicky mají z různých důvodů k dispozici. V případě některých jurisdikcí (mj. i v ČR) je pak mají povinnost uchovávat za účelem jejich využití v trestním řízení.

Technickou výhodou této varianty je, že není nutné rozšíření specifických aplikací mezi obyvatelstvem a dodržování pravidel pro efektivní využití aplikace (např. mít zapnutý energeticky relativně náročný Bluetooth). Ve výsledku je tak tato varianta umožňující sledovat pohyb konkrétního mobilního zařízení v prostoru využitelná k trasování.

[130] Viz GPS tracking with Mapy.cz application. *Observatory of Public Sector Innovation*, publikováno 5. 5. 2020.

Z hlediska prvotního posouzení dopadů je však nutné konstatovat, že riziko nepřiměřeného zásahu do práva na soukromí je v případě této varianty vysoké.

Tato varianta se objevila v Brazílii (kde bylo její využití následně zrušeno Nejvyšším soudem), JAR (*COVID-19 Tracing Database*) a Korejské republice.

Sběr a předávání informací orgánům veřejné správy za účelem trasování. Ze všech variant trasování kontaktů je tato nejméně technologická a nejvíce se podobá manuálnímu dohledávání kontaktů. V základu tato varianta spočívá v zaznamenávání identity zákazníků pracovníky určitých typů provozoven (hotely, restaurace). Pro efektivnější a rychlejší zpracování je k zaznamenávání často využíváno QR kódů.

Výhoda tohoto řešení spočívá v lokalizovaném nasazení na předem určená místa, kde je předpokládán větší výskyt rizikových kontaktů. Druhou výhodou tohoto řešení pak je, že zákazníci nemusí mít instalovanou speciální aplikaci, kterou by museli využívat.

Tento způsob trasování byl využit v Austrálii (v Novém Jižním Walesu), kde byla využívána aplikace provozovaná veřejným sektorem, která byla rovnou propojena s databází, prostřednictvím které trasování probíhalo. Obdobnou funkci plnily také ve Velké Británii používané aplikace *NHS Test and Trace*, *Protect Scotland* nebo *StopCOVID NI*. Podobným nástrojem, který se však ukázal jako relativně nefunkční a byl po krátké době zrušen, bylo posílání SMS propustek v Ruské federaci. Tyto propustky posílali obyvatelé vybraných oblastí, pokud chtěli opustit bydliště.

3.2.2. Statusové certifikáty

Druhým často využívaným typem technologie byly statusové certifikáty. Ty byly používány jako doklad o tom, že jedinec splňuje požadavky stanovené zákonodárcem nebo regulátorem pro přístup na vymezená místa nebo účast na hromadných akcích. Typicky se jednalo o potvrzení, že nositel certifikátu prodělal infekci, byl očkován nebo že byl negativně testován na přítomnost koronaviru SARS-CoV-2.

Z technického hlediska byly certifikáty často součástí dalších aplikací (např. čínský *Health Code* mohl být integrován i do běžně používaných aplikací *WeChat* nebo *Alipay*), vyskytovaly se však i specializované aplikace určené primárně pro uchovávání a kontrolu certifikátů (např. *EU Digitální COVID certifikát* nebo japonská *COVID-19 Vaccination*

Certificate Application). Praktické nasazení certifikátů směřovalo k umožnění rozvolnění omezení pohybu v případech, kdy bylo minimalizováno riziko závažnějších následků pandemie (omezení rizika přenosu nebo omezení rizika těžšího průběhu představujícího zátěž pro zdravotní systém). Vytvoření funkčního systému certifikátů samozřejmě předpokládá důsledný design celé služby, kde primární roli musí hrát zajištění ochrany zpracovávaných osobních údajů z hlediska jejich důvěrnosti, integrity i dostupnosti.

Českým příkladem tohoto technologického řešení byla aplikace *Tečka*, který byla kompatibilní se systémem *EU Digitální COVID certifikát.* [131]

3.2.3. Bezkontaktní služby

Třetím typem identifikovaných technologických řešení je rozvoj bezkontaktních služeb. Jedná se o širokou paletu nástrojů, které směřují k omezení kontaktu mezi lidmi (a v důsledku tedy ke snížení rizika přenosu nákazy). Tento typ má spíše podpůrný efekt, který ale může nakonec pomoci s mírněním dopadů opatření omezujících svobodu pohybu. Specifikem této skupiny technologie je, že výskyt technologických řešení často nebyl iniciován přímo státem, ale objevil se jako reakce společnosti na pandemickou situaci.[132]

Jako příklad řešení tohoto typu je možné uvést rozmach bezhotovostních plateb[133] a používání QR kódů.[134] Jde o nástroje, které jsou primárně zakotvené ve fyzickém světě, ale jejich široká dostupnost snižuje riziko kontaktu a tím i přenosu nákazy. Druhým příkladem jsou nástroje umožňující virtualizaci činností a procesů, které by jinak probíhaly fyzicky, ať už se jedná o široké rozšíření nástrojů pro online setkávání[135] nebo o migraci

[131] Viz Validační aplikace čTečka a Tečka · Covid Portál. *Covid Portál*, citováno k 26. 10. 2022.

[132] V některých omezených případech však byl státem iniciován, například doručování léků a potravin lidem v izolaci bezpilotními prostředky v některých oblastech ČLR.

[133] Viz COVID-19 Drives Global Surge in use of Digital Payments. *World Bank*, publikováno 29. 6. 2022.

[134] QR code usage statistics 2022: 443% scan increase and 438% generation boost. *QRTIGER,* publikováno 31. 8. 2022.

[135] Služba Zoom v prosinci 2019 vykázala průměrně 10 milionů setkání denně, zatímco v dubnu 2020 tato hodnota naskočila na 300 milionů denně. Viz KARL, Katherine A., Joy V. PELUCHETTE, Navi AGHAKHANI. Virtual Work Meetings During the COVID-19 Pandemic: The Good, Bad, and Ugly. *Small Group Research*, 2022, roč. 53 č. 3, s. 343–365.

vzdělávacího systému do online prostředí.[136] Pokud omezení svobody pohybu chápeme jako omezení možnosti jedince zapojovat se do veřejného života a využívat služeb a výdobytků společnosti,[137] tak právě dostupnost nástrojů virtualizované komunikace může tento deficit překonat. Samozřejmě ne zcela dokonale, nicméně může tím přispět k pozitivnímu hodnocení ústavnosti kroků vedoucích k omezení pohyb.

3.2.4. Informování a edukace veřejnosti

Čtvrtým typem využívání technologií je jejich využití za účelem zajištění informovanosti a edukace veřejnosti o probíhající pandemii. Pro účinné nasazení protiepidemických opatření, ať již právních nebo technických, je nezbytné, aby byli lidé o těchto opatřeních, a o jejich smyslu, informování. Jedná se tak primárně o podpůrný nástroj, který může zvýšit pozitivní dopad dalších technických nebo právních nástrojů. Vzhledem k tomu, že součástí testu proporcionality je také hodnocení empirických skutečností (včetně efektivity hodnoceného řešení), mohou technická řešení usnadňující informování a edukaci veřejnosti napomoci k pozitivnímu právnímu hodnocení konkrétní technologie.

Analýza používaných technologií ukázala, že tento typ užití se jen zřídka vyskytoval izolovaně. Za jistou výjimku je možné považovat britskou *COVID Symptom Study*, která umožňovala obyvatelům zaznamenávat symptomy své a svých blízkých. V Japonsku byly rovněž nasazeny samostatné aplikace s čistě informativním charakterem, např. poskytovaly informace o nejbližším testovacím místu, o přijatých opatřeních nebo o průběhu onemocnění covid-19.

Častější však byla přítomnost informační vrstvy v aplikacích, které primárně sloužily k trasování nebo k uchování statusových certifikátů. Příkladem je brazilská aplikace *Coronavírus-SUS*, která kromě Bluetooth trasování nabízela informace o symptomech a prevenci nebo mapu zdravotnických zařízení. Podobně fungovala korejská *Self-*

[136] MUÑOZ-NAJAR, Alberto a kol. *Remote Learning During COVID-19: Lessons from Today, Principles for Tomorrow*. The World Bank, 2022, s. 1–63.

[137] Více viz hodnocení lockdownu jako rizika pro porušení osobní svobody ve VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 125–128.

quarantine Safety Application, která usnadňovala samodiagnostiku a sledování symptomů. Informační složku měla i česká *eRouška*.

Třetím příkladem využití technologie k informování a edukaci jsou bezpilotní prostředky vybavené reproduktory. Jejich prostřednictvím mohly úřady informovat obyvatele, ke kterým by se informace jinak dostávaly obtížně. Tento nástroj tak byl využíván zejména státy se specifickou geografickou či demografickou situací (Brazílie, Čína, JAR).

3.2.5. Dohled a vynucování omezujících opatření

Posledním typem jsou technologie sloužící dohledu a vynucování protiepidemických opatření. Využívání technologií pro efektivnější dohled není novinkou, kterou by přinesla pandemie.[138] Není proto překvapivé, že můžeme sledovat poměrně širokou škálu různých variant. Automatizovaný dohled a vynucování opatření může obecně bezpochyby pomoci s efektivním výkonem práva, a tedy i se zajištěním efektivity kroků směřujících ke zvládnutí krizové situace.[139] Na druhé straně však hrozí značný zásah do jiných práv a právem chráněných zájmů dotčených osob. Může se jednat o zásah do práva na soukromý a rodinný život nebo o otázku přehnaného vynucování pravidel (*overenforcement*), což je situace, kdy jsou předepsaná pravidla vymáhána formalisticky a vedou k zásahu do dalších lidských práv.[140] Nezbytným předpokladem pro nasazení jakéhokoli prostředku sloužícího pro dohled a vynucování opatření je důsledné naplnění zásad a požadavků ochrany osobních údajů. Jde totiž, téměř bez výhrad, o vysoce rizikové zpracování, které vede k rozhodování o právech a povinnostech subjektů údajů. Příkladem, jak by nasazení technologie nemělo vypadat, je situace z Moskvy, kde byla data z aplikace, která fungovala jako nástroj pro dohled nad dodržováním karantén, chybně vyhodnocována. V důsledku tak byly sankcionovány také osoby, které se ničím neprovinily.

[138] Jako příklad za všechny je možné uvést automatizovaná zařízení měřící rychlost na pozemních komunikacích.

[139] Zde pracujeme s předpokladem, že pravidla pro zvládání pandemické situace jsou nastavena správně.

[140] Srovnej např. *Europe: Policing the pandemic: Human rights violations in the enforcement of COVID-19 measures in Europe,* Amnesty International, 2020, s. 1–35.

V rámci tohoto typu využití technologie jsme identifikovali šest dílčích variant využívajících různá technická řešení. Ta se nutně liší jak náročností aplikace, tak mírou zásahu do kolidujících práv a zájmů dotčených osob.

Využívání neanonymizovaných provozních a lokalizačních údajů. První variantou technického řešení pro efektivní dohled a vynucování omezujících opatření je sledování osob prostřednictvím neanonymizovaných provozních a lokalizačních údajů. Podobně jako v případě využití těchto metadat pro trasování kontaktů, i zde hovoří ve prospěch této varianty zejména to, že v mnoha státech jde o již existující systém využívaný pro vyšetřování trestné činnosti.

Zároveň je však nutné dodat, že možnost nakládání s těmito údaji je právně velmi výrazně omezena. Např. česká právní úprava výslovně vyjmenovává instituce, kterým mají poskytovatelé elektronických komunikaci povinnost provozní a lokalizační údaje předávat,[141] a za jakých okolností může k předání dojít.[142] Ústavní soud sice rozhodl, že současná úprava plošného sběru a využívání těchto údajů za účelem vedení trestního řízení je ústavně konformní. Soudní dvůr Evropské Unie ale opakovaně uvádí, že hromadný, plošný, preventivní a nediskriminační sběr těchto údajů odporuje právu na ochranu soukromého a rodinného života a právu na ochranu osobních údajů, která garantují čl. 7 a 8 Listiny základních práv Evropské Unie. Ústavně konformní využití této varianty tak představuje složitý problém.[143]

Kromě plošného sledování celé populace je tuto variantu možné využít ke sledování konkrétních osob, kterým byla nařízena izolace či karanténa.

Využívání anonymizovaných provozních a lokalizačních údajů. Druhá varianta je v základu podobná shora uvedené první variantě, a společně s ní může těžit z již existující povinnosti poskytovatelů elektronických komunikací uchovávat provozní a lokalizační údaje. Jedná se proto o technicky snadno dostupná metadata, která mohou nést

[141] Viz § 97 zákona č. 127/2005 Sb., o elektronických komunikacích.

[142] Viz např. § 88a zákona č. 141/1961 Sb., trestní řád.

[143] Jde např. o rozsudek SDEU ze dne 21. prosince 2016 ve věci C-203/15 - Tele2 Sverige, rozsudek SDEU ze dne 6. října 2020 ve věci C-511/18 - La Quadrature du Net a další, rozsudek SDEU ze dne 2. března 2021 ve věci C-746/18 - Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques).

významnou informační hodnotu pro vyhodnocování průběhu pandemie. Zároveň však v rámci této varianty nebude docházet k tak zásadnímu zásahu do práv dotčených osob, protože se data analyzují po předchozí anonymizaci. V principu tak nemůže jít o vymáhání zaměřené na konkrétní jedince, ale o zjištění vzorců chování ve společnosti. Takovéto využití technologie je vhodné použít pro kontrolu, zda nastavená omezující opatření vyvolávají kýžený efekt (snížení mobility) nebo zda vyžadují další úpravu.

Příkladem je geolokační aplikace *InLoco* (Brazílie), která mapovala pohyb lidí ve specifických oblastech. Aplikace pracovala s anonymizovanými agregovanými daty, která neumožňovala identifikaci osob.

Mobilní aplikace pro kontrolu dodržování nařízené karantény. Třetí variantu pro dohled nad nařízenou izolací nebo karanténou představují mobilní aplikace. K nařízení izolace (či karantény) může dojít v souvislosti se vstupem do země nebo v souvislosti s prokázaným výskytem SARS-CoV-2 u osoby.

Výhodou této varianty je možnost přesného zacílení opatření na okruh osob. Použitá aplikace pak může být vhodně nastavena tak, aby nedocházelo k velmi invazivnímu konstantnímu sledování polohy uživatele, ale aby se osoba například musela v určitých intervalech předepsaným způsobem ohlásit. Druhou výhodou je možnost propojení aplikace s dalšími funkcemi, jako je například uložení statusových certifikátů nebo poskytnutí informačního servisu. Výzvou pochopitelně bude technické nastavení celého procesu provozu aplikace, protože půjde o vysoce rizikové zpracování osobních údajů. Zřejmou nevýhodou pak je nutnost používat pro využití určitých technických řešení kompatibilní chytrý mobilní telefon. Některé státy tuto nevýhodu adresovaly zapůjčením zařízení osobě, které byla nařízena karanténa či izolace.

Příkladem tohoto přístupu je komplexní aplikace *Health Code* (ČLR), která v části svého rozsahu sloužila právě kontrole dodržování karanténních či izolačních opatření. Dalším příkladem je *OEL* (Japonsko) určená ke sledování dodržování povinné karantény při příjezdu do země. V Korejské republice ke kontrole povinné karantény při příjezdu do země sloužila aplikace *Smart Quarantine System*. Tamtéž byla nasazena *Self-quarantine Safety Application*, která prostřednictvím GNSS lokalizovala uživatele a tím kontrolovala dodržování karantény. Podobný nástroj byl nasazen rovněž v Ruské federaci, kde aplikace

požadovala přístup k velkému množství údajů o zařízení (záznamy telefonátů, záznamy z kamery). Kromě značného zásahu do chráněných práv byla aplikace zatížena i chybným vyhodnocováním shromážděných dat.

Jiné technologické prostředky pro kontrolu dodržování nařízené karantény. Čtvrtá varianta je velmi podobná variantě předcházející. Podstatným rozdílem je způsob implementace, kdy nedochází k využití aplikace na chytrém telefonu. Namísto toho jsou využity standardní technické prostředky speciálně vytvořené pro účel kontroly dodržování omezujících opatření. Může se jednat např. o náramky ke kontrole pohybu při uděleném trestu domácího vězení. Výhodou je možnost obejít podmínku vlastnictví chytrého telefonu. Nevýhodou pak je nižší flexibilita v použití.

Náramky pro sledování pohybu osob s nařízenou karanténou byly zavedeny v Korejské republice. Po jisté míře kontroverze bylo jejich použití nakonec podmíněno souhlasem sledované osoby.

Využívání bezpilotních prostředků. Pátou variantou využití technologií za účelem dohledu a vynucování protiepidemických opatření je využívání dronů. Nasazení této technologie úzce souvisí s činností policejních složek. Výhodou je bez pochyby flexibilita využití a možnost efektivního pokrytí značného prostoru (samozřejmě v závislosti na senzorickém vybavení neseném bezpilotními prostředky).

Tato varianta byla využita prakticky ve všech námi sledovaných státech. V Austrálii byla pomocí dronů kontrolována uzavřená hranice mezi státy Viktoria a Nový Jižní Wales. Policejní složky Západní Austrálie pomocí dronů doručovaly upozornění na porušení omezujících opatření. V Brazílii byly drony využity k upozorňování občanů, kteří se účastnili zakázaných shromáždění. ČLR je pak využila jako nástroj pro kontrolu dodržování zavedených opatření. Limitovaného užití se dronům dostalo i v EU, např. v Bulharsku. Zřejmě největší pozornosti se bezpilotním prostředkům dostalo v souvislosti s jejich užitím ve Velké Británii, kde byly používány ke sledování osob za pomoci systémů umožňující rozpoznání registračních značek. Tímto docházelo ke kontrole dodržování opatření omezujících vnitrostátní pohyb.

Využívání kamerových systémů. Šestou variantu použití technologie za účelem dohledu a vynucování omezujících opatření představuje využívání kamerových systémů.

Tato varianta se vyskytuje zejména v zemích, které byly již před příchodem pandemie známé zvýšenou mírou sledování veřejného prostoru kamerovými systémy (často navíc ve spojení s nástroji umožňujícími rozpoznávání obličejů). V rámci omezujících opatření umožnilo nasazení kamerových systémů kombinaci sledování veřejného prostoru (a tím zajištění vymáhání pravidel omezujících pohyb), měření teplot obyvatel (za účelem identifikace potenciálně nakažených osob) a v určitých případech i sledování konkrétních osob (za účelem ověření, zda dodržují nařízená karanténní či izolační opatření).

Příkladem využití této technologie je systém nasazený v ČLR, který spočíval v nasazení dálkových teploměrů, které byly propojeny s kamerovými systémy a umožňovaly rozpoznávání obličejů. Kamery s rozpoznáváním obličejů byly rovněž nasazeny v Ruské federaci (konkrétně v Moskvě), kde došlo k propojení některých zvláštních aplikací s existujícím kamerovým systémem. Soubor nástrojů pak byl využíván pro kontrolu zákazu vycházení. Kamerové systémy snímající teplotu byly nasazeny rovněž ve Velké Británii (velká mezinárodní letiště, přístav Portsmouth). Shromážděná data měla být propojena se systémem rozpoznávání obličejů, což by znamenalo poměrně zásadní zásah do chráněných práv za situace, kdy nebyla jasná účinnost těchto opatření. Ke kontrole dodržování společenského odstupu byly využity kamerové systémy např. v Londýně, Oxfordu, Manchesteru, Cambridge a Nottinghamu.

4. Požadavky na proporcionální nasazení technologických řešení

4.1. Obecné podmínky a předpoklady pro zajištění ústavnosti opatření

Tato kapitola představuje výsledky analýzy nasazení jednotlivých typů technologických opatření a představí je v kontextu různých časových úseků průběhu pandemie. Zaměří se přitom na hlavní obrysy možných zásahů do základních lidských práv s akcentem na právo na ochranu soukromého a rodinného života a na ochranu osobních údajů. Dříve než přistoupíme k analýze konkrétních variant technologií, je nutné zdůraznit obecné principy a podmínky, které je nutné reflektovat vždy. Budou totiž vytvářet základní rámec pro zajištění ústavnosti aplikace konkrétních technologií. Nejedná se striktně pouze o podmínky právní, ale i etické, neboť ty nám pomáhají lépe formulovat jednotlivá východiska v testu proporcionality ve fázi porovnávání kolidujících práv. Obecným podmínkám je věnována tato podkapitola.

Při nasazení jakékoli technologie hrozící zasáhnout do základních práv je nezbytné provést vyhodnocení proporcionality zásahu oproti právům a zájmům. Ty můžeme formulovat jako cíle, které má hodnocené řešení zasahující do základních práv naplnit. V kontextu zvládání pandemie můžeme identifikovat dva základní cíle a s nimi související práva a zájmy: (i) minimalizace dopadů pandemie na společnost a s tím související veřejný zájem na zajištění veřejného zdraví, a (ii) minimalizace nebo vyloučení dopadů způsobených opatřeními omezujícími svobodu pohybu. Jak jsme uvedli výše v metodologické části, našim základním metodologickým východiskem je provedení testu proporcionality. Ten se ve své ryzí podobě skládá ze tří kroků: (i) testu vhodnosti, při kterém je posuzováno, zda dané opatření může dosáhnout deklarovaného cíle, (ii) testu potřebnosti, kdy zjišťujeme, zda neexistuje jiné opatření, které by daného cíle dosáhlo efektivněji, a (iii) samotného pověřování kolidujících práv a zájmů, které je založené na empirických a hodnotových skutečnostech. Dále se zaměříme na skutečnosti, které je specificky nutné v případě hodnocení technických řešení brát při testu proporcionality v potaz.

Základní otázkou testu vhodnosti je uvážení, zda navrhovaná technologie může vůbec dosáhnout deklarovaného cíle. Při vyhodnocení je třeba zvážit níže uvedené okolnosti.

V jaké fázi průběhu pandemie je nasazení technologie zvažováno? Dle odpovědi se bude konkrétní formulace cíle nutně lišit. Zřejmým je pak dílčí závěr, že technologie, která je proporcionální v kontextu zabránění importu nákazy, nemusí být proporcionální ve fázi nelokalizovaného šíření agens, a naopak.

Je technické řešení vědecky podložené a dostatečně přesné? Lze předpokládat, že bude efektivní?[144] Tato otázka zahrnuje řadu dílčích kroků. V prvé řadě by mělo být řešení založeno na vědeckém poznání a na ověřitelných důkazech.[145] Čím více bude známo o mechanismech fungování konkrétní epidemie, tím větší důraz musí být kladen na zahrnutí těchto poznatků do parametrů daného technologického řešení. Dále musí být hodnocené řešení natolik přesné, aby dopadalo na zamýšlené regulované subjekty a aby byla zároveň vyloučena nepřesná práce s daty, která by vedla k nesprávnému využití technologie a nežádoucím dopadům na práva a zájmy obyvatel. Konečně pak je třeba zvážit, jak se odpověď na první otázku testu proporcionality změní, pokud bude technologie nasazena pouze v omezeném rozsahu (např. v důsledku nízké míry akceptace společností). Zcela určitě můžeme dojít k závěru, že mnohá řešení, která „na papíře" vypadají dobře, nebudou v praxi dostatečně efektivní. V důsledku toho nebude jejich nasazení proporcionální, protože neprojdou prvním krokem testu proporcionality.[146]

Je řešení integrováno do širšího kontextu opatření pro zvládání krize? Sekalala uvádí, že *„po digitálních nástrojích, které nabízejí sledování příznaků nebo trasování kontaktů, musí následovat rychlé testování, izolace nebo karanténa, léčba a v případě potřeby následná opatření."*[147] Samotná trasovací aplikace bez návaznosti na další kroky celého systému

[144] Viz též MORLEY, Jessica, Josh COWLS, Mariarosaria TADDEO, Luciano FLORIDI. Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems. *SSRN,* 2020, s. 3.

[145] SEKALALA, Sharifah, Stéphanie DAGRON, Lisa FORMAN, Benjamin Mason MEIER. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 13.

[146] Viz MORLEY, Jessica, Josh COWLS, Mariarosaria TADDEO, Luciano FLORIDI. Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems. *SSRN,* 2020, s. 4.

[147] Viz SEKALALA, Sharifah, Stéphanie DAGRON, Lisa FORMAN, Benjamin Mason MEIER. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 14.

deklarovaného cíle nedosáhne a nemůže tedy projít ani prvním krokem testu proporcionality.[148]

Umožňuje technické řešení zmírnění omezení svobody pohybu? Toto je podpůrná otázka, zaměřená na druhý výše formulovaný cíl. Je zřejmé, že budou řešení, která motivaci ke zmírnění omezení svobody pohybu mít primárně nebudou (zejména taková, která jsou určená k vymáhání existujících omezujících opatření). I v takovém případě však může dojít k pozitivnímu efektu, protože při efektivním vymáhání specificky zacílených opatření nemusí být přikročeno k plošným zákazům a omezením.

V rámci druhého kroku testu proporcionality, tedy testu potřebnosti, bude ověřováno, zda neexistuje méně invazivní řešení. I zde je nutné zvážit řadu okolností, které jsou uvedeny níže.

Je nastavení hodnoceného řešení od základu takové, že maximálně šetří práva dotčených osob? Tato úvaha umožňuje určitou flexibility v nastavování parametrů. Zároveň jde ruku v ruce se základními zásadami ochrany osobních údajů, které právě na minimalizaci rizika zásahu směřují.[149]

Je hodnocené řešení dočasné? Typicky zde budeme zjišťovat, zda v jeho rámci existuje ustanovení o skončení platnosti (*sunset clause*). Požadavek vychází ze zásady omezení zpracování osobních údajů, dle které je nezbytné osobní údaje smazat po naplnění účelu zpracování. Na obecnější úrovni tento požadavek hraje ještě důležitější roli. Je třeba vycházet z předpokladu, že nasazování technických opatření za účelem zvládání pandemie je v principu reakcí na nastalou krizi. Pokud doposud výjimečné řešení způsobuje zásah do práv, nesmí se z něj stát nový setrvalý (standardní) stav. Existence ustanovení o skončení platnosti je tak pro uznání ústavnosti hodnoceného řešení zcela zásadní.[150]

---

[148] Shodně viz CHIUSI, Fabio, Naomi APPELMAN, Rosamunde VAN BRAKEL a kol. *Tracing The Tracers 2021 report: Automating COVID responses.* AlgorithmWatch, 2021.

[149] Shodně viz závěry zprávy Rady Evropy *Digital Solutions to Fight Covid-19. 2020 Data Protection Report*. Council of Europe. 2020, s. 1–36.

[150] Shodně viz SEKALALA, Sharifah, Stéphanie DAGRON, Lisa FORMAN, Benjamin Mason MEIER. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 14.

Dále MORLEY, Jessica, Josh COWLS, Mariarosaria TADDEO, Luciano FLORIDI. Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems. *SSRN,* 2020, s. 3.

Nevyvolává hodnocené řešení diskriminační následky? Při nastavování parametrů fungování konkrétního technického řešení je nezbytné pamatovat, že byť je rozšíření technologií v současné společnosti značné, není rovnoměrné.[151] Nevhodné nastavení parametrů nebo souvisejících procesů může vést k opomenutí zranitelných skupin obyvatel se ztíženým přístupem k technologiím (nízkopříjmové skupiny obyvatel, osoby důchodového věku apod.).[152]

Třetí krok testu proporcionality představuje samotné hodnocení a zvážení kolidujících práv a zájmů. Tento krok bude záviset zejména na závažnosti krizové situace, intenzitě zásahu do relevantních práv, vyhodnocení, zda není zasaženo přímo jádro těchto práv nebo na míře předpokládaného snížení zásahu do práva na svobodu pohybu.

Nad rámec výše uvedených podmínek je třeba uvést dva obecné požadavky, které hrají roli napříč všemi uvedenými kroky testu proporcionality.

Je hodnocené řešení zákonné? Intenzita požadavku na zákonnost řešení se bude lišit podle toho, zda se jedná o nařízené (či alespoň doporučované) řešení, které je zaváděno v rozsahu výkonu státní správy a řízení krizové situace shora, nebo zda jde o technické řešení vznikající spontánně zdola. V prvním případě se nastavování parametrů řešení řídí zásadou legality[153] a je proto nezbytné striktně dodržet požadovaný proces (včetně řádného odůvodňování opatření). Ve druhém případě se základní rámec bude řídit zásadou legální licence, dle které je možné činit vše, co zákon nezakazuje.

Má hodnocené řešení důvěru společnosti?[154] V širším pojetí se může jednat o důvěru společnosti v systematická řešení ze strany státu jako taková či o důvěru v politické vedení státu, že si s krizí dokáže poradit. Nízká důvěra v řešení totiž bezpochyby povede k nižší

---

[151] Více ke konceptu „digital divide“ např. DIJK, Jan van. *The digital divide*. First published. Cambridge: Polity, 2020. V kontextu zdravotnictví pak specificky viz SUN, Nina a kol. Human Rights and Digital Health Technologies. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 21–32.

[152] Viz SEKALALA, Sharifah, Stéphanie DAGRON, Lisa FORMAN, Benjamin Mason MEIER. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 15.

[153] Viz čl. 2 odst. 3 Ústavy (1/1993 Sb.): *„Státní moc slouží všem občanům a lze ji uplatňovat jen v případech, v mezích a způsoby, které stanoví zákon.“*

[154] Viz HOGAN, Katie, Briana MACEDO, Venkata MACHA, Arko BARMAN, Xiaoqian JIANG. Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation. *JMIR Medical Informatics*, 2021, roč. 9, č. 7, e27449.

míře přijetí a tím i k nižší účinnosti (potenciálně až ústavní nekonformitě, protože nižší účinnosti způsobí neschopnost dosáhnout deklarovaného cíle). K zajištění této zcela nezbytné důvěry může pomoci řada kroků, jako je například důkladné informování i probíhající krizi a o rizicích s ní spojených, vysvětlování nezbytnosti přijímaných opatření a transparentnosti fungování nasazovaných technických řešení.[155] Součástí informační kampaně pak musí být i cílené snižování obav veřejnosti z rizik spojených se zásahem do soukromí a se zpracováním osobních údajů.[156]

Výše uvedené tvoří základní požadavky pro nasazení jakýchkoli technických řešení, u kterého dochází ke středu základních práv. Tvoří také rámec, který je třeba mít na paměti při vyhodnocování možností aplikace konkrétních technologií a jejich dopadů na kolidující práva, jenž je prováděno v následujících podkapitolách této zprávy. V těch budou poskytnuta vodítka pro provedení testu proporcionality u výše identifikovaných typů technologických řešení (a eventuálně jejich dílčích variant). Každý typ (a varianta) bude zhodnocen v kontextu časových úseků šířící se epidemie a cílů reakce, které se k nim váží.

Pro rekapitulaci, jednotlivé časové úseky jsou následující.[157]

- Nástup agens (úsek 1). Cílem je zabránění či pozdržení importu do země.
- Lokalizované šíření agens (úsek 2). Cílem je zabránění či pozdržení importu do dalších oblastí nebo komunit.
- Nelokalizované šíření agens (úsek 3). Cílem je zpomalení šíření nákazy v populaci.
- Návrat k běžnému chodu (úsek 4). Cílem je postupné uvolňování omezujících opatření v návaznosti na zlepšující se epidemiologickou situaci.

[155] Viz SEKALALA, Sharifah, Stéphanie DAGRON, Lisa FORMAN, Benjamin Mason MEIER. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 15–16.

[156] Viz CHAN, Eugene Y., Najam U. SAQIB. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, 2021, roč. 119, s. 106718.

[157] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 140–141.

4.2. Trasování kontaktů

4.2.1. Hodnocení jednotlivých variant

Nástroje využívající protokol Bluetooth pro detekci zařízení s nainstalovanou aplikací v blízkém okolí. Trasovací aplikace využívající technologii Bluetooth představují při vhodném technickém provedení jen velmi malé riziko pro právo na ochranu soukromí a ochranu osobních údajů. Je tomu tak z důvodu, že pracují se silně pseudonymizovanými údaji, které není možné použít k určení konkrétního pohybu uživatele. Při správném nastavení v rámci širšího kontextu protiepidemických opatření a při dostatečném přijetí aplikace společností může nasazení technologie v této variantě pomoci při zachycení šíření nákazy. Nízká rizikovost zpracování osobních údajů napomáhá při testu proporcionality ve prospěch použití této varianty. Je však nutné upozornit na kritiku, která analyzuje zkušenosti z nasazení technologie v různých částech světa. V praxi se totiž ukázalo, že využití této technologie často nenaplňuje přísliby, které provázely její spuštění.[158]

V prvním časovém úseku není použití této varianty vhodné, protože není způsobilé naplnit cíle, které jsou s tímto časovým úsekem spojené (zabránění či pozdržení importu do země).

Ve druhém časovém úseku je nasazení technologie vhodné díky nízké rizikovosti nepřekračující ústavní limity, pokud je provedeno cíleně v kontextu zasažených komunit. Příkladem může být nasazení Bluetooth náramků u pracovníků v přístavu v Antverpách. Plošné nasazení by bylo nepřiměřené.

Ve třetím časovém úseku je nasazení této varianty trasovacích aplikací vhodné za splnění obecných předpokladů uvedených v této zprávě (kap. 4.1). Pro efektivní nasazení je nezbytné zajistit významné rozšíření v rámci populace, dosáhnout vysoké důvěry v řešení a zajistit provázání na další fáze procesu řízení epidemie. V takovém případě může široké

[158] Dobrým příkladem je nasazení v Austrálii (viz výše). Dále viz např. WHITE, Lucie, Philippe VAN BASSHUYSEN. Without a trace: Why did corona apps fail? *Journal of Medical Ethics*, 2021, roč. 47, č. 12.

Také CHIUSI, Fabio, Naomi APPELMAN, Rosamunde VAN BRAKEL a kol. *Tracing The Tracers 2021 report: Automating COVID responses*. AlgorithmWatch, 2021.

nasazení technologie v této variantě přispět k mírnějším opatřením omezujícím svobodu pohybu.

Ve čtvrtém časovém úseku je nasazení technologie proporcionální v případě komunit, ve kterých vlna epidemie stále doznívá. Je však nutné průběžně sledovat data a od mandatorního využívání ustoupit, jakmile není nezbytné.

Zaznamenávání pohybu zařízení v prostoru prostřednictvím mobilní aplikace a GNSS. Trasovací aplikace využívající přesnou geolokalizaci zařízení a jejího uživatele sledují stejný cíl, jako trasovací aplikace využívající protokolu Bluetooth. Je tedy, na základě jejich dat, možné určit blízkost rizikového kontaktu a na základě toho pokračovat s dalšími úkony (nařízení testování apod.). Na rozdíl od předcházející varianty je riziko asociované se zpracováním osobních údajů tímto způsobem vyšší. Jsou totiž uchovávány údaje o lokalitě, ze kterých je možné sledovat pohyb zařízení a jeho uživatele – tato varianta pracuje s absolutními hodnotami umístění, nikoli pouze s relativními hodnotami blízkosti k jinému zařízení s nainstalovanou aplikací. Při neopatrném nakládání s daty je možné získat celou řadu informací o soukromém a rodinném životě uživatele.

Vzhledem k tomu je v případech, kdy by připadalo v úvahu použití trasovací varianty využívající Bluetooth, nutné uzavřít, že řešení využívající GNSS neprojde přes druhý krok testu proporcionality (kritérium potřebnosti). Ve specifických případech (a pouze v těchto případech), kdy by nebylo objektivně možné využít variantu využívající Bluetooth, bude vyhodnocení možnosti nasazení v různých úsecích průběhu epidemie analogické se závěry předcházející varianty.

Zaznamenávání pohybu zařízení v prostoru s využitím provozních a lokalizačních údajů. Podobně jako v případě předcházející varianty, i zde dochází k zaznamenávání místa výskytu a pohybu mobilních zařízení a tím pádem i jejich uživatelů. Hlavní rozdíl spočívá v tom, že tato varianta nevyžaduje od jednotlivců instalaci aplikace, ale je možné využít metadata shromažďovaná a uchovávaná poskytovateli služeb elektronických komunikací. Z toho důvodu je teoreticky možné vynutit nasazení této varianty i v případech, kdy by byla přítomna větší míra nedůvěry či nechuti společnosti, která by se projevovala v nízké míře používání trasovacích aplikací. Na druhou stranu je nutné dodat, že aby byl naplněn účel nasazení této varianty, bylo by využití metadat k trasování nutné v celospolečenském

měřítku. Jednalo by se o značný zásah do práva na ochranu soukromí a ochranu osobních údajů, který by dle našeho názoru postihnul jádro těchto práv. Tato varianta tak neprojde testem proporcionality v žádném časovém úseku probíhající epidemie.

Sběr a předávání informací orgánům veřejné správy za účelem trasování. Manuální záznamy o pohybu osob, ať už jsou shromažďovány elektronicky a zaznamenávány do centralizované databáze nebo jsou prováděny lokálním záznamem (např. kniha hostů), představují potenciální zásah do práva na ochranu soukromí a ochranu osobních údajů. Při splnění předpokladů správného nastavení procesů zpracování (tj. zabezpečení, minimalizace údajů, omezená doba zpracování, přístup pouze oprávněnými osobami apod.) však toto riziko není vysoké. Podmínkou pro efektivní nasazení (a tedy i kladný výsledek testu proporcionality) je navázání na další procesy určené k řešení epidemie (např. povinné testování).

Výhodou této varianty je možnost přesného zacílení na místa, která jsou v daném momentě vyhodnocena jako riziková. Může se jednat o restaurace, hotely nebo třeba prostředky městské hromadné dopravy, jejichž užití může být podmíněno např. využitím QR kódu pro evidenci přítomnosti ve vymezeném prostoru v konkrétním časovém úseku. Druhou výhodou pak je, že striktně vzato nejsou na osoby kladeny nároky na využívání technologií (např. dokument s osobním QR kódem je možné nosit vytištěný). Tím jsou omezena rizika plynoucí z diskriminace některých skupin obyvatel (*digital divide*).

Obecně je o této variantě možné uvažovat jako o ústavně konformní. Je však nutné opět zdůraznit, že nezbytnou podmínkou pro tento závěr je splnění obecných předpokladů uvedených výše (kap. 4.1).

V prvním časovém úseku není využití varianty vhodné, protože nemůže naplnit cíle, které jsou s tímto časovým úsekem spojené (zabránění či pozdržení importu do země).

Ve druhém časovém úseku je nasazení technologie možné a díky nízké rizikovosti nebude překračovat ústavněprávní limity, pokud bude provedeno cíleně v kontextu rizikových míst v zasažených komunitách či oblastech. V tomto směru může výrazně prospět jako nástroj umožňující přijetí menších restrikcí omezujících svobodu pohybu.

Ve třetím časovém úseku je nasazení této varianty možné a v konkrétních kontextech vhodné. Máme za to, že její nasazení by se mohlo doplňovat s plošným trasováním za pomoci technologie Bluetooth. Synergickým efektem společného nasazení by mohlo dojít k potlačení některých nevýhod obou variant.

Ve čtvrtém časovém úseku je nasazení technologie proporcionální v komunitách, v nichž epidemie doznívá. Je však nutné upustit od plošného mandatorního využití ve chvíli, kdy není zcela nezbytné.

4.2.2. Přehledová tabulka variant

Varianta	Riziko zásahu do práva na ochranu soukromí a osobních údajů	Nástup agens (úsek 1)	Lokalizované šíření agens (úsek 2)	Nelokalizované šíření agens (úsek 3)	Návrat k běžnému chodu (úsek 4)
Bluetooth	Nízké	Nevhodné (nenaplní cíl)	Vhodné, je-li lokalizované a zacílené na oblasti výskytu agens	Vhodné, je-li nasazeno korektně a jsou splněny obecné požadavky	Možné ponechat v komunitách, kde je nasazení stále nezbytné (vyžaduje pravidelnou kontrolu nezbytnosti)
GNSS	Střední	Nevhodné (nenaplní cíl)	Nevhodné (neprojde kritériem potřebnosti, pokud je možné nasadit variantu Bluetooth)	Nevhodné (neprojde kritériem potřebnosti, pokud je možné nasadit variantu Bluetooth)	Nevhodné (neprojde kritériem potřebnosti, pokud je možné nasadit variantu Bluetooth)
Provozní a lokalizační údaje	Vysoké	Nevhodné (hrozí zásah do jádra práva na ochranu soukromí)	Nevhodné (hrozí zásah do jádra práva na ochranu soukromí)	Nevhodné (hrozí zásah do jádra práva na ochranu soukromí)	Nevhodné (hrozí zásah do jádra práva na ochranu soukromí)
Sběr a předávání údajů za účelem trasování	Nízké	Nevhodné (nenaplní cíl)	Vhodné, je-li zacílené na oblasti výskytu agens a rizikové prostory (vhodné jako limitace omezení svobody pohybu)	Vhodné, je-li nasazeno korektně a jsou-li splněny obecné požadavky (vhodné jako doplněk k variantě Bluetooth)	Možné ponechat v komunitách, kde je nasazení stále nezbytné (vyžaduje pravidelnou kontrolu nezbytnosti)

4.3. Statusové certifikáty

Statusové certifikáty byly využívány jako doklad splnění požadavků stanovených zákonodárcem či regulátorem pro přístup na vymezená místa či účast na veřejných akcích. Hlavním cílem tohoto nástroje je umožnit přijetí mírnějších opatření omezujících svobodu pohybu. Aplikace pro správu certifikátů může být samostatně stojící nebo propojená s jinými (např. trasovacími) aplikacemi. Z hlediska hodnocení dopadů statusových certifikátů na základní práva a oprávněné zájmy tento rozdíl nehraje roli.

Ve své abstraktní podobě využívání statusových certifikátů nepředstavuje vysoké riziko zásahu do práva na ochranu soukromí nebo osobních údajů. V kontextu praktického nasazení se však může jednat o rizikové zpracování osobních údajů – ať už z důvodu, že jsou statusovým certifikátem zpracovávány údaje o zdravotním stavu (zvláštní kategorie osobních údajů dle čl. 9 GDPR) nebo proto, že na základě tohoto zpracování bude rozhodováno o právech a povinnostech osob (např. umožnění nebo naopak znemožnění vstupu).

Z těchto důvodů je zcela nezbytné, aby byl při vytváření certifikátových aplikací zajištěn vysoký standard ochrany osobních údajů nejenom ve vztahu k zabezpečení, ale k celému komplexu právních povinností plynoucích z GDPR. Navázané riziko vytvoření diskriminačního prostředí také není zcela zanedbatelné. Zavedení statusových certifikátů musí být důkladně podloženo výsledky vědeckého a empirického poznání o chování a průběhu epidemie. Pro snížení rizika vytvoření diskriminačního prostředí je nezbytná maximální jistota, že umožnění přístupu ke službám pouze osobám s konkrétním statusem (doloženým statusovým certifikátem) bude mít zamýšlený efekt na protiepidemické cíle. Případné riziko nedostupnosti aplikací s certifikáty pro určité skupiny obyvatel lze řešit vytištěním certifikátu nebo navázaného QR kódu.

Za podmínky vyřešení uvedených výzev může být tento nástroj ústavně konformní a může vést ke snížení míry restrikce spojené s opatřeními omezujícími svobodu pohybu.

V prvním časovém úseku mohou být na základě certifikátů osoby vpouštěny na území státu, jedná se tak o opatření schopné dosáhnout cíle.

Ve druhém časovém úseku umožní technologie využívání služeb v zasažených lokalitách, které tak nebudou muset být plošně uzavřeny.

Ve třetím časovém úseku, kdy je nejvíce pravděpodobné a proporcionální mandatorní plošné nasazení technologie, je v důsledku umožněno využívání služeb v celostátním měřítku. Ty tak nebudou muset být plošně uzavřeny.

V průběhu čtvrtého časového úseku je nasazení technologického řešení možné, je však třeba silně dbát na prevenci diskriminace při postupně slábnoucí vlně šíření agens.

4.4. Bezkontaktní služby

Tento typ technologií má podpůrný efekt. Zavedení bezkontaktních služeb nicméně snižuje riziko nákazy a může tedy zásadně pomoci zmírnit opatření omezující svobodu pohybu. Riziko zásahu do jiných práv samozřejmě není možné zcela vyloučit, ale při dodržování základních právních povinností (např. povinností správce osobních údajů dle GDPR) je možné jej vyhodnotit jako nízké.

Například v rámci nasazení QR kódů pro bezkontaktní platby nebo identifikaci osob hrozí riziko zásahu do práva na ochranu osobních údajů v případě zneužití nepovolanou osobou. Další hrozby mohou představovat kyberbezpečnostní rizika (např. využití QR kódů jako vektoru útoku na mobilní zařízení[159]). V případě nástrojů pro online setkávání pak může riziko spočívat v protiprávním zpracování osobních údajů provozovateli těchto služeb. Obecné riziko pak představuje hrozba diskriminace související zejména s vyloučením určitých skupin obyvatel z využívání služby v důsledku nízké digitální gramotnosti. Pokud však jsou tato rizika pro vývoji opatření aktivně adresována, je riziko neproporcionálního zásahu do práv minimální.

Tento závěr pak platí pro všechny časové úseky vývoje pandemie, ve kterých může zavedení bezkontaktních služeb snížit množství epidemiologicky významných (rizikových) kontaktů a nemusí tak dojít k přijetí opatření výrazně omezujících svobody pohybu.

[159] Viz např. NAIK, Bhavesh. QR Code: USSD attack. *INFOSEC*, publikováno 29. 5. 2013.

4.5. Informování a edukace veřejnosti

Podobně jako v předcházejícím případě mají nástroje k určené informování a edukaci společnosti spíše podpůrný efekt. Ten spočívá ve snaze zajistit, aby díky dostatečné informovanosti, obeznámenosti s problémem a budování důvěry v poskytovaná řešení byli obyvatelé více ochotni dodržovat opatření a také využívat nástrojů (např. trasovacích aplikací) s reálným dopadem. Hodnocení rizik zásahu do práva na ochranu soukromí a osobních údajů je podobné jako v předchozím případě. Byť tato rizika samozřejmě nelze zcela vyloučit, budou kontextová vzhledem k povaze použitého nástroje. Pokud aplikace například umožňuje sledování symptomů uživatele a na základě toho pomáhá vyhodnocovat průběh jeho onemocnění, půjde o zpracování zvláštní kategorie osobních údajů podle čl. 9 GDPR. Při nastavování procesů těchto technologických nástrojů pak musí jejich tvůrci důsledně pamatovat na obecná pravidla ochrany osobních údajů (pokud jsou osobní údaje zpracovávány) a na riziko související s nižší digitální gramotností některých skupin obyvatel. Pokud tvůrce tyto aspekty řádně vyhodnotí a zahrne je do procesu tvorby aplikace, je riziko zásahu do práv a zájmů dotčených osob minimální. Tento závěr pak opět platí pro všechny časové úseky vývoje epidemie.

4.6. Dohled a vynucování omezujících opatření

4.6.1. Hodnocení jednotlivých variant

Využívání neanonymizovaných provozních a lokalizačních údajů. Se zpracováním provozních a lokalizačních údajů se pojí vysoké riziko zásahu do práva na ochranu soukromí a osobních údajů. Využití těchto údajů v neanonymizované podobě k plošnému sledování a kontrole dodržování opatření omezujících svobodu pohybu by znamenalo zásah do jádra práva na ochranu soukromí. Snadná technická proveditelnost takového sledování pak nemůže sloužit jako argument pro uskutečnění zpracování. Existující právní úprava jasně vymezuje, za jakých okolností je možné s těmito údaji nakládat. Opětovně je pak nutné zmínit existenci ustálené judikatury SDEU, která na využívání těchto údajů pohlíží kriticky právě s poukazem na značnou intenzitu zásahu do chráněných práv

subjektů údajů. Problémem této varianty je také nízká transparentnost zpracování osobních údajů, což opět hovoří proti jejímu nasazení.[160]

Specifickou úpravou využití této varianty by bylo její zacílení na konkrétní osoby, u kterých by individuální okolnosti mohly takovýto zásah odůvodnit. Typicky se může jednat o osoby, kterým byla nařízena karanténa. Zde je možné uvažovat o přiměřenosti využití existujících mechanismů *data retention* k dohledu nad dodržováním opatření a není tak nutné řešení okamžitě odmítnout pro zjevnou nepřiměřenost zásahu. Následně však bude nutné vzít v potaz další aspekty ovlivňující test proporcionality. Bude se jednat zejména o závažnost šířených agens (resp. závažnost nemoci, kterou vyvolávají). Pokud půjde o onemocnění, které by svojí závažností (nebezpečnost, nakažlivost) nedosahovala dostatečné intenzity, převážil by zájem na ochraně soukromí a tuto variantu by nebylo možné použít. Jinými slovy, v rámci našeho hodnocení nevylučujeme možnost implementace této varianty za situace, kdy není možné zajistit dozor a vymáhání jiným (do práv méně zasahujícím) způsobem, a zároveň představuje šířící se agens zcela zásadní riziko.

V prvním časovém úseku je možné obecně přijmout nasazení této technologie na kontrolu osob vstupujících na území státu, kterým byla nařízena karanténa, pokud není technicky možné tento dozor provést jinak. Rozsah aplikace této varianty je tak velmi omezen. Je nutné zdůraznit, že podmínkou pro konstatování ústavnosti nasazení této varianty je zásadně vysoká rizikovost šířeného agens a navázaného onemocnění.

Ve druhém časovém úseku je opět možné obecně přijmout nasazení této varianty na dozor nad osobami, kterým byla nařízena karanténa. Znovu se jedná o cílené nasazení technologie. I zde je podmínkou pro závěr o ústavnosti této varianty nutné konstatovat (i) nedostupnost alternativního nástroje pro dozor a (ii) vysoké riziko spojené se šířením agens a navázaného onemocnění.

Třetí časový úsek nepředstavuje dle našeho názoru vhodnou dobu pro nasazení této varianty dozoru. Efektivní naplnění cíle tohoto úseku (omezení šíření agens v populaci) by

[160] Viz rozsudek SDEU ze dne 21. prosince 2016 ve věci C-203/15 - Tele2 Sverige, rozsudek SDEU ze dne 6. října 2020 ve věci C-511/18 - La Quadrature du Net a další, rozsudek SDEU ze dne 2. března 2021 ve věci C-746/18 - Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques).

zřejmě vyžadovalo plošné (nediskriminační, necílené) nasazení. To by představovalo zásah do jádra práva na ochranu soukromí a osobních údajů.

Naopak čtvrtý časový úsek by nasazení této varianty ve vymezených případech umožňoval. Jednalo by se např. o nutnost zabránit spuštění další vlny šíření za situace, kdy by neexistoval jiný (méně invazivní) způsob, jak dozor zajistit.

Využívání anonymizovaných provozních a lokalizačních údajů. V případě využití anonymizovaných dat můžeme obecně konstatovat nižší riziko zásahu do práva na ochranu soukromí a ochranu osobních údajů. Složky státu, které vymáhají opatření, totiž nesledují pohyb konkrétních lidí, ale vysoké koncentrace osob na jednom místě, což může vypovídat o porušování opatření omezujících svobodu pohybu. Výhodou tohoto řešení je jeho nezávislost na vůli a ochotě obyvatel k jeho využívání (není nutné využívání aplikace). Při řádném nastavení celého procesu (včetně dostatečně důkladné anonymizace metadat) bude riziko zásahu této varianty do práv a chráněných zájmů nízké.

Při využívání této varianty je nutné dbát na odlišnosti v míře anonymizace dat mezi hustě a řídce osídlenými oblastmi. Zatímco v množství zařízení ve městech lze anonymitu subjektu údajů většinou předpokládat, v rurálních oblastech nikoli. To platí zejména, pokud jsou metadata uchovávána a následně analyzována za delší časové období. Důvodem je, že v řídce osídlených oblastech je prostřednictvím analýzy vzorců chování (*patterns of life analysis*) jednodušší údaje deanonymizovat. V rámci analýzy se předpokládá, že majitel zařízení následuje vzorce běžného rytmu života a na základě korelace těchto vzorců můžeme vyvozovat závěry o jeho identitě a aktivitách. Typicky tam, kde zařízení zůstává po celou noc, lze předpokládat místo bydliště. Stejná lokalita výskytu v průběhu pracovních dní pak bude pravděpodobně místem zaměstnání. V řídce osídlených oblastech nelze samotnou anonymizaci považovat za dostatečnou ochranu práva na soukromí a osobních údajů subjektů – vzhledem k okolnostem (menší hustotě osídlení) je zde anonymizace přirozeně méně robustní. Bez dalších opatření (např. dobrovolnost užití, kratší horizont uchovávání, využití pouze pro automatizovanou detekci zvýšené koncentrace zařízení na jednom místě) by tak bylo nutné konstatovat riziko vysokého zásahu do práv.

V prvním časovém úseku není využití technologie vhodné. Nemůže totiž naplnit cíle s tímto úsekem spojené (zabránění nebo pozdržení importu agens do země).

Ve druhém časovém úseku je nasazení vhodné pro monitorování lidí ve vymezených zasažených oblastech. Vzhledem k nasazení v rámci oblasti, kde dochází k lokalizovanému šíření, je dopad do kolidujících práv minimální.

Ve třetím časovém úseku musí docházet k plošnému nasazení technologického řešení. To zvyšuje nároky na správnost a robustnost použitých anonymizačních technik a na zabezpečení zpracovávaných údajů. Pokud jsou tyto podmínky naplněny, zůstává riziko do práva na ochranu soukromí a osobních údajů nízké. Varianta nevytváří atmosféru sledování a nebude tak představovat zásah do jádra práva na soukromí.

Ve čtvrtém časovém úseku je vhodné věnovat pozornost snížení rizika zásahu do kolidujících práv tím, že bude nasazení omezeno pouze na oblasti, kde je vzhledem k epidemiologické situaci (doznívání vlny šíření nákazy apod.) nezbytné.

Mobilní aplikace pro kontrolu dodržování nařízené karantény. Další variantou přispívající k dohledu a vynucování opatření je využívání speciálních aplikací v mobilních zařízeních. Prostřednictvím těchto aplikací pak dochází k dozoru nad osobami, kterým byla nařízena karanténa či izolace. Oproti sledování skrze provozní a lokalizační údaje má tato varianta zásadní výhodu, která snižuje potenciální zásah do práva na ochranu soukromí a osobních údajů. Spočívá v možnosti zajistit takové nastavení konkrétního řešení, které neumožní konstantní sledování osoby. Druhou výhodou je pak obecně vyšší míra transparentnosti probíhajícího sledování.

Nezbytným předpokladem pro ústavně konformní implementaci však zůstávají technické parametry konkrétní aplikace. V jádru se totiž jedná o vysoce rizikové zpracování osobních údajů, které vyžaduje maximální pozornost při naplňování podmínek stanovených právním rámcem ochrany osobních údajů.

Dle našeho názoru by bylo vhodnější toto řešení nenařizovat, ale umožnit jeho dobrovolné užití. Při nasazení této varianty je nutné pamatovat rovněž na potenciální diskriminaci v důsledku *digital divide*. Jakkoli některé státy poskytovaly kompatibilní mobilní zařízení jedincům, kteří je neměli k dispozici, plošné poskytnutí této možnosti není realistické.

V prvním časovém úseku je opatření velmi vhodné pro dozor nad osobami vstupujícími na území státu, kterým byla nařízena izolace či karanténa. Bude se jednat o limitovanou množinu osob, kterým je v nezbytných případech možné poskytnout mobilní zařízení. Tato varianta dle našeho názoru projde všemi kroky testu proporcionality i v případě povinného nasazení (zejména v případě vysoké rizikovosti šířeného agens).

Ve druhém, třetím i čtvrtém časovém úseku je nasazení této varianty možné, protože sleduje žádoucí cíl. Při vhodném nastavení nebude představovat vysoký zásah do kolidujících práv. Vzhledem k citlivé povaze nasazení je nutné doporučit dobrovolné (nikoli mandatorní) užívání.

Jiné technologické prostředky pro kontrolu dodržování nařízené karantény. Tato varianta je velmi podobná variantě předcházející. Liší se pouze v tom, že pro kontrolu jedince jsou využívány technické prostředky vytvořené pro tento účel, například náramky používané v kontextu kontroly dodržování testu domácího vězení. Výhodou tohoto řešení oproti předcházející variantě je, že tyto nástroje často již existují a vzhledem k povaze původního užití splňují vysoké požadavky na ochranu osobních údajů. Související nevýhodou je obtížná možnost plošného nasazení této varianty.

V prvním časovém úseku je opatření vhodné pro dozor nad osobami vstupujícími na území státu, kterým byla nařízena izolace či karanténa. Bude se jednat o limitovanou množinu osob, a omezené množství dostupných zařízení nemusí představovat zásadní překážku. I v tomto případě máme za to, že v případě vysokého rizika spojeného se šířením agens je v principu možné tuto variantu nařídit.

Ve druhém časovém úseku je nasazení této varianty možné, protože sleduje žádoucí cíl a při vhodných parametrech použití nebude představovat vysoký zásah do kolidujících práv. Vzhledem k citlivé povaze je vhodné tuto variantu nenařizovat, ale umožnit využití na bázi dobrovolnosti. Oproti mobilním aplikacím může být problém se zajištěním dostatečného množství zařízení.

Ve třetím časovém úseku není nasazení opatření vhodné, protože velmi pravděpodobně neumožní dosáhnout cíle s ohledem na rozsáhlé šíření agens a očekávaný nedostatek zařízení. Pouze částečné nasazování (do vyčerpání zásob) by nebylo účelné a bylo by interpretováno jako diskriminační.

Ve čtvrtém časovém úseku je nasazení této varianty opět vhodné, pokud bude omezeno na oblasti, kde je nasazení nezbytné. Vzhledem k citlivé povaze je vhodné tuto variantu nenařizovat, ale umožnit využití na bázi dobrovolnosti. Oproti mobilním aplikacím může být problém se zajištěním dostatečného množství zařízení.

Využívání bezpilotních prostředků. V rámci této varianty jde o zajišťování dohledu na veřejných prostranstvích a do značné míry tak technologie funguje podobně jako existující a poměrně rozšířené kamerové systémy. Stejně jako u nich nasazení této varianty úzce souvisí s činností pořádkových sil. Na obecné úrovni je s nasazením této varianty spojeno riziko zásahu do práva na ochranu soukromí a osobních údajů. Je nezbytné, aby bylo toto riziko posouzeno v kontextu konkrétní situace. Bezpilotní letouny je tak dle našeho názoru možné využívat například pro kontrolu dodržování opatření omezujících svobodu pohybu, zejména v případě srocování větších skupin lidí, pokud není k dispozici méně invazivní prostředek. Jako vhodné se jeví použití bezpilotních prostředků nad neobydlenými hraničními oblastmi, pokud existuje riziko, že by mohly být využity k zakázanému přeshraničnímu pohybu. I to je však závislé na konkrétní situaci – nasazení pro dozor nad hranicemi v průběhu nelokalizovaného šíření na území státu může být neproporcionální, protože již není způsobilé naplnit stanovený cíl (zabránit nebo odložit zavlečení agens). Jako problematické se také ukázalo využívání termokamer pro identifikaci osob se zvýšenou teplotou – jde totiž o zpracování údajů o zdravotním stavu (zvláštní kategorie osobních údajů dle čl. 9 GDPR), které jsou navíc neprůkazné co do identifikace nakažených osob.

V kontextu nasazení bezpilotních prostředků je třeba upozornit na dvě limitní situace, kde by dle našeho názoru docházelo k zásahu do jádra práva na ochranu soukromí a osobních údajů. Prvním je vybavení bezpilotních prostředků systémem automatického rozpoznávání obličejů. Druhým je plošné nasazení dronů k dozoru a vymáhání zákazu vycházení. Obě situace by vedly k vytváření atmosféry neustálého sledování a jednalo by se o zjevně neproporcionální nasazení této varianty.

V průběhu prvního úseku je cílené nasazení dronů za účelem kontroly dodržování opatření v jasně vymezených lokalitách proporcionální, pokud neexistuje varianta méně invazivního dozoru (např. v podobě statické kamery). Vhodné místo je například dozor nad rozlehlejšími neobydlenými prostory v okolí státních hranic.

V průběhu druhého úseku je cílené nasazení dronů za účelem kontroly dodržování opatření v jasně vymezených lokalitách proporcionální za situace, kdy neexistuje varianta méně invazivního dozoru (např. v podobě statické kamery). Bezpilotní prostředky nesmí být nasazeny v rozsahu, který by dal vzniknout pocitu neustálého sledování. Drony dále nesmí být použity pro identifikaci obličejů a sběr a vyhodnocování dalších biometrických údajů.

V rámci třetího úseku je cílené nasazení dronů proporcionální za situace, kdy neexistuje varianta méně invazivního dozoru, a pokud je lokální nasazení dronů vzhledem k naplnění cíle dostatečné. Drony opět nesmí být použity v rozsahu, který vede ke vzniku pocitu neustálého sledování, a k identifikaci obličejů nebo dalších biometrických projevů.

Čtvrtý úsek je vhodný pro cílené nasazení dronů za účelem kontroly dodržování omezujících opatření v jasně vymezených lokalitách (resp. nasazení bude proporcionální), pokud neexistuje méně invazivní varianta dozoru (např. v podobě statické kamery). Drony nesmí být použity na identifikaci obličejů. Je třeba dbát na to, aby nasazení bezpilotních prostředků v lokalitách nebylo diskriminační.

Využívání kamerových systémů. Pro kamerové systémy platí v zásadě stejné podmínky, které jsou uvedené výše u varianty s využitím bezpilotních prostředků. Podstatným rozdílem je, že kamerové systémy mohou představovat relativně menší riziko zásahu v souvislosti se svojí statickou povahou. Toto riziko nicméně stále existuje a velikost tohoto rizika může být ovlivněna konkrétními parametry využití kamerových systémů. Stejně jako u dronů je nutné vyloučit napojení kamerového systému na funkci automatického rozpoznává obličejů, případně na nástroje umožňující identifikaci jedince pomocí jiných biometrických znaků. Takové využití by totiž dle našeho názoru zcela jistě představovalo zásah do jádra práva na ochranu soukromí a osobních údajů. Stejně problematické je využívání kamerových systémů na sledování pohybu konkrétních vozidel prostřednictvím rozpoznávání registračních značek. Jakékoli nasazení kamerových systémů pak musí splnit vysoké požadavky na zajištění ochrany osobních údajů.

V průběhu prvního úseku je možné nasazení kamerových systémů na letištích, hraničních přechodech, přístavech a dalších místech, přes která probíhá vstup osob na území státu. V kontextu tohoto nasazení je možné u závažných onemocnění předpokládat

proporcionalitu nasazení termokamer za účelem odhalení osob se zvýšenou teplotou, pokud je známo, že zvýšená teplota je jednoznačným symptomem nemoci vyvolávané zájmovým agens. Na detekci osoby se zvýšenou teplotou samozřejmě musí navazovat systém dalších procesů, které dokáží na detekci zvýšené teploty reagovat (např. nařízení testování, izolace) – není proporcionální snímat teplotu samonosně bez existence následných mechanismů reakce. Pro proporcionální nasazení této varianty je pak nezbytné, aby odpovídalo poznatkům o působení nemoci způsobované sledovaným agens. Pokud by se zvýšená teplota vyskytovala jen v menším procentu případů, nasazení by nebylo efektivní, a proto by bylo nepřiměřené. Po skončení první fáze přestává být tato varianta proporcionální, protože jejím nasazením není možné nadále dosáhnout cíle prvního úseku (zabránění nebo zpomalení zavlečení agens).

V průběhu druhého úseku je cílené nasazení kamerových systémů za účelem kontroly dodržování omezujících opatření v jasně vymezených lokalitách proporcionální. Kamery nesmí být použity na automatickou identifikaci obličejů a dalších biometrických projevů.

Ve třetím úseku je cílené nasazení kamerových systémů za účelem kontroly dodržování opatření v jasně vymezených lokalitách proporcionální, pokud je lokální nasazení kamerových systémů k naplnění cíle dostatečné. Kamery nesmí být použity pro automatickou identifikaci obličejů a dalších biometrických projevů.

Ve čtvrtém úseku je cílené nasazení kamerových systémů za účelem kontroly dodržování opatření v jasně vymezených lokalitách proporcionální. Kamery nesmí být použity k automatické identifikaci obličejů a dalších biometrických projevů. Je nutné dbát, aby stanovení lokalit, ve kterých budou kamerové systémy k dozoru využívány, bylo náležitě odůvodněno a nebylo diskriminační.

4.6.2. Přehledová tabulka variant

Varianta	Riziko zásahu do práva na ochranu soukromí a osobních údajů	Nástup agens (úsek 1)	Lokalizované šíření agens (úsek 2)	Nelokalizované šíření agens (úsek 3)	Návrat k běžnému chodu (úsek 4)
Neanonymizované provozní a lokalizační údaje	Velmi vysoké (plošné využívání), vysoké (cílené využívání)	Plošně nevhodné (zásah do jádra práva na ochranu soukromí), cíleně pouze za splnění přísných podmínek	Plošně nevhodné (zásah do jádra na ochranu soukromí), cíleně pouze za splnění přísných podmínek	Plošně i cíleně nevhodné (zásah do jádra na ochranu soukromí)	Plošně nevhodné (zásah do jádra na ochranu soukromí), cíleně pouze za splnění přísných podmínek
Anonymizované provozní a lokalizační údaje	Nízké	Nevhodné (nenaplní cíl)	Vhodné (cílení na oblasti výskytu agens a rizikové prostory)	Vhodné, pokud jsou zajištěny vysoké standardy anonymizace a ochrany osobních údajů	Vhodné (cílení na oblasti výskytu agens a rizikové prostory)
Mobilní aplikace	Střední	Vhodné pro dozor nad osobami s nařízenou karanténou	Vhodné (ideálně na dobrovolné bázi)	Vhodné (ideálně na dobrovolné bázi)	Vhodné (ideálně na dobrovolné bázi)
Jiné prostředky (např. náramky)	Střední	Vhodné pro dozor nad osobami s nařízenou karanténou	Vhodné (ideálně na dobrovolné bázi)	Nevhodné (nízká dostupnost vede k neschopnosti naplnit cíl)	Vhodné (ideálně na dobrovolné bázi)
Bezpilotní prostředky	Střední	Vhodné pro dozor nad neobydlenými úseky státních hranic	Vhodné pouze za splnění přísných podmínek	Vhodné pouze za splnění přísných podmínek	Vhodné pouze za splnění přísných podmínek
Kamerové systémy	Střední	Vhodné pro nasazení na hraničních přechodech	Vhodné pouze za splnění přísných podmínek	Vhodné pouze za splnění přísných podmínek	Vhodné pouze za splnění přísných podmínek

5. Závěr

Výzkumná zpráva *Proporcionalita krizových opatření omezujících svobodu pohybu*[161] představila základní rámec, na který jsme navázali v této výzkumné zprávě. Zásadním poznatkem převzatým z první zprávy bylo rozdělení průběhu epidemie na čtyři časové úseky. Ty se liší v charakteristice šíření agens populací, a tedy i v různých cílech, které je třeba sledovat krizovými či jinými opatřeními usilujícími o zmírnění dopadu epidemie.

V této (druhé) výzkumné zprávě jsme mapovali, jak technologická řešení nasazovaná v průběhu pandemie covidu-19 (způsobeného koronavirem SARS-CoV-2) zasahují do chráněných práv a zájmů dotčených osob, zejména s ohledem na právo na ochranu soukromého a rodinného života (právo na ochranu soukromí) a právo na ochranu osobních údajů. Cílem této zprávy bylo určit dopady technologických nástrojů na tato práva v rámci jednotlivých časových úseků, ve kterých je průběh epidemie možné popsat.

Jako základní ústavní limit pro extenzivní nasazení technologických prostředků přispívajících ke zvládání šíření SARS-CoV-2 bylo určeno právo na ochranu soukromí a právo na ochranu osobních údajů. Obě tato práva byla stručně představena v kap. 2, kde jsme také identifikovali nepřekonatelný limit pro nasazení technologických nástrojů v podobě jádra práva na soukromí. Za zcela neproporcionální (a proto nepřijatelné) jsme označili takové použití technologie, které povede k plošnému a nediskriminačnímu sledování obyvatel, a které bude bránit ve výkonu dalších práv a svobod (*chilling* efekt) garantovaných ústavním pořádkem.

Další limit pro nasazení technologických prostředků tvoří právní režim ochrany osobních údajů. Při využívání technologií pro zvládání šíření agens bude v naprosté většině případů docházet k jejich zpracování. Ochrana osobních údajů jako regulatorní nástroj působí preventivně, a proto svědomitá aplikace těchto pravidel přispěje k souladu s ústavním pořádkem. Při nasazení konkrétní technologie je tak nutné splnit konkrétní povinnosti plynoucí z GDPR a respektovat obecné zásady uvedené v čl. 5 GDPR. Zpracování osobních údajů v kontextu omezení dopadů epidemie ve většině případů spadá do oblasti vysoce

[161] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021.

rizikového zpracování. Vzhledem k tomu je v souladu se zásadou odpovědnosti správce a role hodnocení rizik při zpracování osobních údajů nezbytné, aby byly všechny požadavky i obecné zásady naplňovány svědomitě a precizně. Jedná se o zcela nezbytnou podmínku, bez jejíhož dodržení nemůže nasazení technologického řešení právně obstát, byť by se jinak jádra práva na soukromí netýkalo.

V kap. 3 jsme provedli přehledovou analýzu technologií, které byly využity s cílem ovlivnit průběh pandemie SARS-CoV-2. S variantami využívaných technologických řešení jsme pracovali na abstraktní technické úrovni bez zahrnutí konkrétního společenského a kulturního kontextu, ve kterém byla daná řešení nasazována. Při vytváření přehledu jsme vycházeli z narativních případových studií zpracovaných ve zprávě *Proporcionalita krizových opatření omezujících svobodu pohybu*.[162] Do přehledu jsme zahrnuli pouze podmnožinu států G20, která byla významná z hlediska využitých technologických nástrojů. Našim cílem nebylo podat kvantitativní analýzu četnosti využívání různých technologií, ale získání kvalitativního přehledu možných variant. Náš postup tak nese jisté prvky metody zakotvené teorie. Vzhledem k tomu, že první výzkumná zpráva se zaměřovala na státy G20 v období od 1. ledna 2020 do 30. června 2021, provedli jsme ještě rešerši pro minimalizaci rizika, že jsme v důsledku omezeného časového rámce první zprávy nezařadili typově unikátní technologii.

Tímto postupem jsme identifikovali pět základních typů technologických nástrojů (dvě z nich s variantami) sledujících konkrétní cíle:

1. Trasování kontaktů s variantami využívajícími (i) protokol Bluetooth, (ii) zaznamenávání pohybu pomocí GNSS, (iii) zaznamenávání pohybu využitím provozních a lokalizačních údajů, a (iv) jiný sběr a následné předávání informací orgánům veřejné správy.
2. Statusové certifikáty
3. Bezkontaktní služby
4. Informování a edukace veřejnosti

[162] Viz VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021, s. 14–115.

5. Dohled a vynucování omezujících opatření s variantami využívajícími (i) neanonymizované provozní a lokalizačních údaje, (ii) anonymizované provozní a lokalizační údaje, (iii) mobilní aplikace, (iv) jiné prostředky dohledu (např. náramky), (v) bezpilotní prostředky, a (vi) kamerové systémy.

Následující kap. 4 představovala analytické jádro této zprávy. V její první části jsme identifikovali podmínky, které musí být nezbytně nutně splněny, aby byla zajištěna proporcionalita a ústavnost nasazení technologického opatření. Rovněž jsme v rámci schématu klasického testu proporcionality uvedly u jeho jednotlivých kroků podmínky, které je třeba brát v potaz při vyhodnocování proporcionality nasazovaných technických nástrojů za účelem zvládání epidemie. Zbylé části kap. 4 jsou věnovány analýze možností nasazení identifikovaných technologií (a jejich variant), a určení rizikovosti a intenzity souvisejícího zásahu do práva na ochranu soukromí a osobních údajů. Zahrnuli jsme také vliv jednotlivých fází šíření agens (resp. odlišných cílů, které jsou v jednotlivých úsecích krizovými opatřeními sledovány).

Jako technologie, které nejsou za žádných okolností vhodné k nasazení z důvodu jejich zásahu do jádra práva na ochranu soukromí a osobních údajů jsme identifikovali:

1. Trasování s využitím provozních a lokalizačních údajů
2. Využití neanonymizovaných provozních a lokalizačních údajů za účelem dohledu nad dodržováním omezujících opatření a jejich vynucování
3. Využívání automatického rozpoznávání obličejů (a dalších biometrických údajů) kamerami umístěnými na bezpilotních prostředcích
4. Plošné nasazování dronů za účelem dohledu nad dodržováním omezujících opatření a jejich vynucování
5. Využívání automatického rozpoznávání obličejů (a dalších biometrických údajů) statickými kamerovými systémy
6. Plošné sledování statickými kamerovými systémy sledujícími pohyb konkrétních vozidel prostřednictvím automatického rozpoznávání registračních značek

Nasazením ostatních technologií je dle našeho názoru možné podepřít mimořádná opatření omezující svobodu pohybu. V důsledky využití technologických prostředků je tak možné efektivněji vymáhat existující opatření omezující svobodu pohybu nebo sáhnout

k mírnějším opatřením při dosažení podobného efektu. Může tak vlastně dojít ke zmírnění dopadů omezujících opatření na svobodu pohybu výměnou za zahrnutí práva na ochranu soukromí a ochranu osobních údajů.

Vzhledem k povaze testu proporcionality, který je vázán na okolnosti konkrétní situace, jsme nemohli poskytnout univerzálně platné odpovědi. Poskytli jsme však vodítka, kterými je nutné se při zavádění technologických prostředků doprovázejících opatření k omezení pohybu řídit.

Ve třetí výzkumné zprávě budeme syntetizovat zjištění výzkumné zprávy *Proporcionalita krizových opatření omezujících svobodu pohybu* a této výzkumné zprávy. Cílem bude předložit doporučení ohledně možných technologických prostředků ke zmírnění ústavněprávního deficitu krizových opatřeních omezujících svobodu pohybu.

Reference

- 10 Ways Technology is Helping To Fight the Coronavirus. *UNDP*, publikováno 27. 2. 2020. Dostupné z: https://www.undp.org/china/blog/10-ways-technology-helping-fight-coronavirus
- About the ZOE COVID Study. *ZOE COVID Study*. Dostupné z: https://covid.joinzoe.com/
- Aplicativo Tô de Olho ajuda a conter o coronavírus no RN. *Secretaria de Estado da Saúde Pública*, publikováno 8. 4. 2020. Dostupné z: https://portalcovid19.saude.rn.gov.br/noticias/aplicativo-to-de-olho-ajuda-a-conter-o-coronavirus-no-rn/
- Australian Government Department of Health and Aged. COVIDSafe app. *Australian Government Department of Health and Aged Care*, publikováno 24. 4. 2020. Dostupné z: https://www.health.gov.au/resources/apps-and-tools/covidsafe-app
- BIENKOV, Adam. UK police officers are using drones to „lockdown shame" people for walking their dogs in remote areas during the coronavirus outbreak. *Business Insider,* publikováno 27. 3. 2020. Dostupné z: https://www.businessinsider.com/coronavirus-uk-police-are-using-drones-to-lockdown-shame-walkers-2020-3
- BODA, Ridwaan. South Africa: Contact tracing and its aftermath. *DataGuidance*, publikováno 8. 9. 2022. Dostupné z: https://www.dataguidance.com/opinion/south-africa-contact-tracing-and-its-aftermath
- BURKI, Talha. China's successful control of COVID-19. *The Lancet Infectious Diseases*, 2020, roč. 20, č. 11, s. 1240–1241. Dostupné z: https://doi.org/10.1016/S1473-3099(20)30800-8
- BRKAN, Maja. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. *German Law Journal*, 2019, roč. 20, č. 6, s. 864–883. Dostupné z: https://doi.org/10.1017/glj.2019.66
- CAVOUKIAN, Ann. *Privacy by Design - The 7 Foundational Principles*. IAPP, 2011, s. 1–12. Dostupné z: https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/
- CLARKE, Roger. Privacy Introduction and Definitions. *Roger Clarke's Web-Site*, publikováno 24. 6. 2016. Dostupné z: http://www.rogerclarke.com/DV/Intro.html
- Coronavirus: EU interoperability gateway for contact tracing and warning apps – Questions and Answers. *European Commission*, publikováno 19. 10. 2020. Dostupné z: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1905
- COVID-19 Drives Global Surge in use of Digital Payments. *World Bank*, publikováno 29. 6. 2022. Dostupné z: https://www.worldbank.org/en/news/press-release/2022/06/29/covid-19-drives-global-surge-in-use-of-digital-payments
- COVID-19 Health System Response Monitor (HSRM): Russian Federation. *European Observatory on Health Systems and Policies*. Dostupné z: https://eurohealthobservatory.who.int/monitors/hsrm/hsrm-countries/hsrm/russian-federation
- COVID-19 Update: NSW Businesses to use Service NSW QR Code. *Australian Institute of Food Safety,* publikováno 29. 12. 2020. Dostupné z: https://www.foodsafety.com.au/news/covid-19-update-nsw-businesses-use-service-nsw-qr-code
- *Digital Solutions to Fight Covid-19. 2020 Data Protection Report*. Council of Europe, 2020, s. 1-36. Dostupné z: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c.
- DIJK, Jan van. *The digital divide*. First published. Cambridge: Polity, 2020.
- DIMITROVA, Aseniya. How drones help cities during the Covid-19 pandemic. *TheMayor.EU,* publikováno 23. 3. 2020. Dostupné z: https://www.themayor.eu/en/a/view/how-drones-help-cities-during-the-coronavirus-pandemic-4631
- EU Digital COVID Certificate. *European Commission*. Dostupné z: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en

- *Europe: Policing the pandemic: Human rights violations in the enforcement of COVID-19 measures in Europe.* Amnesty International, 2020, s. 1-35. Dostupné z: https://policehumanrightsresources.org/policing-the-pandemic-human-rights-violations-in-the-enforcement-of-covid-19-measures-in-europe
- *Emergency Powers and Civil Liberties Report – June 2020*. Big Brother Watch, 2020. Dostupné z: https://bigbrotherwatch.org.uk/wp-content/uploads/2020/07/Emergency-Powers-and-Civil-Liberties-Report-Big-Brother-Watch-June-2020.pdf
- *Emergency Powers and Civil Liberties Report – May 2020*. Big Brother Watch, 2020. Dostupné z: https://bigbrotherwatch.org.uk/wp-content/uploads/2020/06/Emergency-Powers-and-Civil-Liberties-Report-May-2020-Final.pdf
- *Emergency Powers and Civil Liberties Report – October 2020*. Big Brother Watch, 2020. Dostupné z: https://bigbrotherwatch.org.uk/wp-content/uploads/2020/11/Emergency-Powers-and-Civil-Liberties-Report-OCT-2020.pdf
- Encontrar informações atualizadas sobre o coronavírus (Covid-19) — Português (Brasil). *gov.br*, citováno k 15. 7. 2022. Dostupné z: https://www.gov.br/pt-br/servicos/obter-informacoes-atualizadas-sobre-o-corona-virus-covid-19
- FULL SPEECH: Ramaphosa's address to the nation. *Eyewitness news,* publikováno 12. 7. 2020. Dostupné z: https://ewn.co.za/2020/07/12/full-speech-ramaphosa-s-address-to-the-nation
- GELLERT, Raphaël. Understanding the notion of risk in the General Data Protection Regulation. *Computer Law & Security Review*, 2018, roč. 34, č. 2, s. 279–288. Dostupné z: https://doi.org/10.1016/j.clsr.2017.12.003
- GELLERT, Raphaël, Serge GUTWIRTH. The legal construction of privacy and data protection. *Computer Law & Security Review*, 2013, roč. 29, č. 5, s. 522–530. Dostupné z: https://doi.org/10.1016/j.clsr.2013.07.005
- GERDO, Vladimir. Russia Develops Coronavirus Contact-Tracing App. *The Moscow Times*, publikováno 17. 11. 2020. Dostupné z: https://www.themoscowtimes.com/2020/11/17/russia-develops-coronavirus-contact-tracing-app-a72068
- GPS tracking with Mapy.cz application. *Observatory of Public Sector Innovation*, publikováno 5. 5. 2020. Dostupné z: https://oecd-opsi.org/covid-response/gps-tracking-with-mapy-cz-application/
- GRUBB, Ben. Mobile phone location data used to track Australians' movements during coronavirus crisis. *The Sydney Morning Herald*, publikováno 4. 4. 2020. Dostupné z: https://www.smh.com.au/technology/mobile-phone-location-data-used-to-track-australians-movements-during-coronavirus-crisis-20200404-p54h09.html
- GUZMAN, Joseph. China rolls out facial recognition thermometers on buses amid coronavirus outbreak. *TheHill*, publikováno 19. 2. 2020. Dostupné z: https://thehill.com/changing-america/well-being/prevention-cures/483669-china-rolls-out-facial-recognition-thermometers
- HENDRY, Justin. COVIDSafe privacy protections now locked in law. *iTnews*, publikováno 14. 5. 2020. Dostupné z: https://www.itnews.com.au/news/covidsafe-privacy-protections-now-locked-in-law-548119
- HEO, Kyungmoo, Daejoong LEE, Yongseok SEO a kol. Searching for Digital Technologies in Containment and Mitigation Strategies: Experience from South Korea COVID-19. *Annals of Global Health*, 2020, roč. 86, č. 1, art. 109. Dostupné z: http://doi.org/10.5334/aogh.2993
- HOLLÄNDER, Pavel. *Filosofie práva*. 2., rozš. vyd. Plzeň: Čeněk, 2012.
- How Korean mobile apps are making COVID-19 resources more accessible. *GoodUX*. Dostupné z: https://goodux.appcues.com/blog/korean-mobile-apps-coronavirus-covid-19
- How tracing and warning apps can help during the pandemic. *European Commission*. Dostupné z: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/travel-during-coronavirus-pandemic/how-tracing-and-warning-apps-can-help-during-pandemic_en

- HOECKE, Mark Van. Legal Doctrine: Which Method(s) for What Kind of Discipline? In: HOECKE, Mark van, (ed.) *Methodologies of legal research: which kind of method for what kind of discipline?* Oxford, Portland: Hart, 2011, s. 1–18.
- HOGAN, Katie, Briana MACEDO, Venkata MACHA, Arko BARMAN, Xiaoqian JIANG. Contact Tracing Apps: Lessons Learned on Privacy, Autonomy, and the Need for Detailed and Thoughtful Implementation. *JMIR Medical Informatics*, 2021, roč. 9, č. 7, e27449. Dostupné z: https://medinform.jmir.org/2021/7/e27449
- HLOUCH, Lukáš. *Teorie a realita právní interpretace*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2011.
- HUANG, Kristin. Chinese woman charged with organising protests during coronavirus lockdown. *South China Morning Post*, publikováno 19. 4. 2020. Dostupné z: https://www.scmp.com/news/china/politics/article/3080590/coronavirus-lockdown-woman-charged-organising-protests-against
- HUSTINX, Peter. EU Data Protection Law: The Review of Directive 95/ 46/ EC and the General Data Protection Regulation. In: CREMONA, Marise, (ed.). *New technologies and EU law*. First edition. New York: Oxford University Press, 2017, s. 123–173.
- CHAN, Eugene Y., Najam U. SAQIB. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior*, 2021, roč. 119, s. 106718. Dostupné z: https://doi.org/10.1016/j.chb.2021.106718
- CHIUSI, Fabio, Naomi APPELMAN, Rosamunde VAN BRAKEL a kol. *Tracing The Tracers 2021 report: Automating COVID responses*. AlgorithmWatch, 2021. Dostupné z: https://algorithmwatch.org/en/tracing-the-tracers/2021-report/
- CHUNG, Sunghee, Sujin LEE. South Korea: Democracy, Innovation, and Surveillance. In: RAMRAJ, Victor Vridar (ed.). *COVID-19 in Asia: law and policy contexts*. New York: Oxford University Press, 2021, s. 240–250.
- iNews — Police Filming Innocent Members of the Public With Drones and Putting It Online. *Big Brother Watch*, publikováno 27. 3. 2020. Dostupné z: https://bigbrotherwatch.org.uk/2020/03/inews-police-filming-innocent-members-of-the-public-with-drones-and-putting-it-online/
- In Loco adapta sua tecnologia de geolocalização para ajudar no combate à Covid-19. *ABES*, publikováno 12. 4. 2020. Dostupné z: https://abes.com.br/en/in-loco-adapta-sua-tecnologia-de-geolocalizacao-para-ajudar-no-combate-a-covid-19/
- Japan's COVID-19 app failed to pass on some contact warnings. *Reuters*. publikováno 3. 2. 2021. Dostupné z: https://www.reuters.com/article/us-health-coronavirus-japan-app-idUSKBN2A31BA
- Japan launches COVID vaccine certificate app. *Nikkei Asia*, publikováno 20. 12. 2021. Dostupné z: https://asia.nikkei.com/Spotlight/Coronavirus/COVID-vaccines/Japan-launches-COVID-vaccine-certificate-app
- KARL, Katherine A., Joy V. PELUCHETTE, Navi AGHAKHANI. Virtual Work Meetings During the COVID-19 Pandemic: The Good, Bad, and Ugly. *Small Group Research.* 2022, roč. 53 č. 3, s. 343–365. Dostupné z: https://doi.org/10.1177/10464964211015286
- Kamery videonabljuděnija v Moskvě vyjavili boljeje 200 graždan, narušivšich režim samoizoljacii [orig. Камеры видеонаблюдения в Москве выявили более 200 граждан, нарушивших режим самоизоляции]. *TASS* [orig. ТАСС], publikováno 18. 3. 2020. Dostupné z: https://tass.ru/obschestvo/8012841
- KINYILI, Musyoka, Justin B. MUNYAKAZI a Abdulaziz YA MUKHTAR. Mathematical modeling and impact analysis of the use of COVID Alert SA app. *AIMS Public Health*, 2021, roč. 9, č. 1, s. 106–128. Dostupné z: https://doi.org/10.3934/publichealth.2022009
- KLERK, Marize de. Drones Spread Word About COVID-19 in Rural South Africa. *VOA,* publikováno 28. 4. 2020. Dostupné z: https://www.voanews.com/a/covid-19-pandemic_drones-spread-word-about-covid-19-rural-south-africa/6188352.html
- KOOPS, Bert-Jaap a kol. A Typology of Privacy. *University of Pennsylvania Journal of International Law*, 2017, roč. 38, č. 2, s. 483–576. Dostupné z: https://scholarship.law.upenn.edu/jil/vol38/iss2/4/

- Korea to use electronic bracelets on violators of self-isolation rules. *koreatimes*, publikováno 11. 4. 2020. Dostupné z: https://www.koreatimes.co.kr/www/nation/2021/12/356_287714.html
- LANGFORD, Eleanor. Home Office Plans To Use Military-Grade Drones To Pursue Suspects And Monitor Protests Are Raising Privacy Concerns. *Politics Home*, publikováno 17. 9. 2020. Dostupné z: https://www.politicshome.com/news/article/military-grade-drones-home-office
- LÉVY, Pierre. *Becoming virtual: reality in the Digital Age*. New York: Plenum Trade, 1998.
- LIANG, Fan. COVID-19 and Health Code: How Digital Platforms Tackle the Pandemic in China. *Social Media + Society*, 2020, roč. 6, č. 3, s. 1–4. Dostupné z: https://doi.org/10.1177/2056305120947657
- MARI, Angelica. Brazil integrates Apple-Google exposure notification tech into coronavirus app. *ZDNet*, publikováno 5. 8. 2020. Dostupné z: https://www.zdnet.com/article/brazil-integrates-apple-google-exposure-notification-tech-into-coronavirus-app/
- MAKARYCHEV, Andrey, Maria GOES, Anna KUZNETSOVA. The Covid Biopolitics in Russia: Putin's Sovereignty versus Regional Governmentality. *Czech Journal of International Relations*, 2020, roč. 55, č. 4, s. 31–47. Dostupné z: https://doi.org/10.32422/mv-cjir.1729
- MAYNES, Charles. Moscow To Launch New Surveillance App To Track Residents In Coronavirus Lockdown. *NPR*, publikováno 1. 4. 2020. Dostupné z: https://www.npr.org/sections/coronavirus-live-updates/2020/04/01/825329399/moscow-launches-new-surveillance-app-to-track-residents-in-coronavirus-lockdown
- MEDINA-PEREA, Itzelle A. Do contact-tracing apps have a future? *The Conversation*, publikováno 16. 3. 2022. Dostupné z: http://theconversation.com/do-contact-tracing-apps-have-a-future-177283
- MÍŠEK, Jakub. *Moderní regulatorní metody ochrany osobních údajů*. Brno: Masarykova univerzita, 2020.
- MOLLA, Alemayehu a Stan KARANASIOS. The COVIDSafe app is dead. What can we learn from this „failure"? *The Conversation*, publikováno 12. 8. 2022. Dostupné z: http://theconversation.com/the-covidsafe-app-is-dead-what-can-we-learn-from-this-failure-188582
- MORLEY, Jessica, Josh COWLS, Mariarosaria TADDEO, Luciano FLORIDI. Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems. *SSRN*, 2020, s. 1–6. Dostupné z: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3582550
- MUÑOZ-NAJAR, Alberto a kol. *Remote Learning During COVID-19: Lessons from Today, Principles for Tomorrow*. The World Bank, 2022, s. 1-63. Dostupné z: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/160271637074230077/Remote-Learning-During-COVID-19-Lessons-from-Today-Principles-for-Tomorrow
- NAIK, Bhavesh. QR Code: USSD attack. *INFOSEC*, publikováno 29. 5. 2013. Dostupné z: https://resources.infosecinstitute.com/topic/qr-code-ussd-attack/
- OSUMI, Magdalena. How Japan tracks arrivals from abroad to curb the spread of new virus strains. *The Japan Times*, publikováno 29. 3. 2021. Dostupné z: https://www.japantimes.co.jp/news/2021/03/29/national/japan-coronavirus-tracking-app/
- PENNEY, Jonathon. Chilling effects and transatlantic privacy. *European Law Journal*, 2019, roč. 25, č. 2, s. 122–139. Dostupné z: https://doi.org/10.1111/eulj.12315
- QR code usage statistics 2022: 443% scan increase and 438% generation boost. *QRTIGER,* publikováno 31. 8. 2022. Dostupné z: https://qrcode-tiger.com/qr-code-statistics-2022-q1
- REIMAN, Jeffrey H. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 1976, roč. 6, č. 1, s. 26–44. Dostupné z: https://www.jstor.org/stable/2265060
- Río de Janeiro usa drones con altavoces para dispersar las aglomeraciones durante la pandemia. *La Vanguardia*, publikováno 15. 4. 2020. Dostupné z: https://www.lavanguardia.com/internacional/20200415/48547778010/rio-janeiro-usa-drones-altavoces-dispersar-aglomeraciones-pandemia.html
- ROACH, April. AI cameras being used on UK streets to monitor social distancing. *Evening Standard*, publikováno 8. 10. 2020. Dostupné z: https://www.standard.co.uk/news/uk/ai-cameras-london-social-

distancing-rules-a4566446.html

- Russia uses facial recognition to tackle virus. *BBC News,* publikováno 4. 4. 2020. Dostupné z: https://www.bbc.com/news/av/world-europe-52157131
- Russia: Intrusive Tracking App Wrongly Fines Muscovites. *Human Rights Watch*, publikováno 21. 5. 2020. Dostupné z: https://www.hrw.org/news/2020/05/21/russia-intrusive-tracking-app-wrongly-fines-muscovites
- RYŠAVÝ, Zdeněk. Amnesty International tvrdě kritizuje uzavírání romských osad na Slovensku a v Bulharsku. *Romea.cz*, publikováno 20. 4. 2020. Dostupné z: https://romea.cz/cz/zaostreno/amnesty-international-tvrde-kritizuje-uzavirani-romskych-osad-na-slovensku-a-v-bulharsku/
- SEKALALA, Sharifah, Stéphanie DAGRON, Lisa FORMAN, Benjamin Mason MEIER. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 7–20. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7762901/
- SCHNEIDER, Florian, Rogier CREEMERS a kol. *How Asia Confronts COVID-19 through Technology*. The Leiden Asia Centre, 2021. Dostupné z: https://scholarlypublications.universiteitleiden.nl/access/item%3A2965785/view
- SILVA, Ken. Brazilian court declares data protection a fundamental right in landmark decision. *Global Data Review*, publikováno 11. 5. 2020. Dostupné z: https://globaldatareview.com/article/brazilian-court-declares-data-protection-fundamental-right-in-landmark-decision
- SMITS, Jan M. *The mind and method of the legal academic*. Cheltenham, UK: Edward Elgar, 2012.
- SOLOVE, Daniel J. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 2006, roč. 154, č. 3, s. 477–564. Dostupné z: https://doi.org/10.2307/40041279
- SOLOVE, Daniel J. Conceptualizing Privacy. *California Law Review*, 2002, roč. 90, č. 4, s. 1087–1155. Dostupné z: https://doi.org/10.2307/3481326
- SOO LINDBERG, Kari a Colum MURPHY. Drones Take to China's Skies to Fight Coronavirus Outbreak - Bloomberg. *Bloomberg*, publikováno 4. 2. 2020. Dostupné z: https://www.bloomberg.com/news/articles/2020-02-04/drones-take-to-china-s-skies-to-fight-coronavirus-outbreak
- SUN, Nina a kol. Human Rights and Digital Health Technologies. *Health and Human Rights Journal*, 2020, roč. 22, č. 2, s. 21–32. Dostupné z: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7762914/
- STEVENS, Robert. Russia's coronavirus app is turning it into a police state. *Decrypt*, publikováno 2. 4. 2020. Dostupné z: https://decrypt.co/24348/russia-app-coronavirus-government-surveillance
- TANGERMANN, Victor. In China, this coronavirus app pretty much controls your life. *Futurism*, publikováno 16. 4. 2020. Dostupné z: https://futurism.com/contact-tracing-apps-china-coronavirus
- The end of South Africa's state of disaster and lockdown restrictions is coming. *BusinessTech*, publikováno 10. 12. 2021. Dostupné z: https://businesstech.co.za/news/government/545726/the-end-of-south-africas-state-of-disaster-and-lockdown-restrictions-is-coming/
- THORN, Adam. Drones to guard NSW-Vic border as Melbourne locks down. *Australian Aviation,* publikováno 7. 7. 2020. Dostupné z: https://australianaviation.com.au/2020/07/drones-to-guard-nsw-vic-border-as-melbourne-locks-down/
- TINGLE, Rory. 1,000 AI scanners are monitoring how close pedestrians are walking. *Mail Online,* publikováno 9. 10. 2020. Dostupné z: https://www.dailymail.co.uk/news/article-8822715/1-000-AI-scanners-monitoring-close-pedestrians-walking-other.html
- Validační aplikace čTečka a Tečka · Covid Portál. *Covid Portál*, citováno k 26. 10. 2022. Dostupné z: https://covid.gov.cz/situace/ockovani/validacni-aplikace-ctecka-tecka
- VIEIRA ALONSO, Fabio, Carolina BARBOSA DE L. CUNHA V DA COSTA. The impact of Covid-19 for data protection in Brazil: the perspective of Brazil's supreme court. *International Bar Association.* Dostupné z: https://www.ibanet.org/article/82B25A81-7422-4F07-AAA8-9C2DB19E22AF
- VOGT, Florian a kol. Effectiveness evaluation of digital contact tracing for COVID-19 in New South Wales, Australia. *The Lancet Public Health*. 2022, roč. 7, č. 3, s. e250–e258. Dostupné z:

https://doi.org/10.1016/S2468-2667(22)00010-X

- VYHNÁNEK, Ladislav, Anna BLECHOVÁ, Michael BÁTRLA, Jakub MÍŠEK, Tereza NOVOTNÁ a Jakub HARAŠTA. *Proporcionalita krizových opatření omezujících svobodu pohybu*. Brno: Masarykova univerzita pro Ministerstvo vnitra České republiky, 2021. 173 s. Dostupné z: https://is.muni.cz/publication/1815657/cs/Proporcionalita-krizovych-opatreni-omezujicich-svobodu-pohybu/
- WA police to use drones to enforce coronavirus restrictions. *9News*, publikováno 30. 3. 2020. Dostupné z: https://www.9news.com.au/national/coronavirus-outbreak-wa-police-to-use-drones-to-enforce-restrictions/30387b30-f34d-40bd-84af-479cd10ff9fe
- WANG, Zhiqiong June, Jianfu CHEN. People's Republic of China: Legal Response to Covid 19. In: KING, Jeff, Octavio FERRAZ (eds.). *The Oxford Compendium of National Legal Responses to Covid-19*. Oxford University Press, 2021. Dostupné z: https://oxcon.ouplaw.com/view/10.1093/law-occ19/law-occ19-e22
- WAGNEROVÁ, Eliška. Kde má být svoboda, tam musí být soukromí. In: ŠIMÍČEK, Vojtěch (ed.) *Právo na soukromí*. Brno: Masarykova Univerzita, Mezinárodní Politologický Ústav, 2011, s. 49–62.
- WAGNEROVÁ, Eliška. Čl.4 (Limity omezování základních práv). In: WAGNEROVÁ, Eliška, Vojtěch ŠIMÍČEK, Tomáš LANGÁŠEK, Ivo POSPÍŠIL aj. *Listina základních práv a svobod: Komentář* [Systém ASPI]. Wolters Kluwer, 2012.
- WARREN, Samuel D. a Louis D. BRANDEIS. The Right to Privacy. *Harvard Law Review*, 1890, roč. IV, č. 5, s. 193–220. Dostupné z: https://www.jstor.org/stable/1321160?seq=3#metadata_info_tab_contents
- WESTIN, Alan F. *Privacy and freedom*. New York: Atheneum, 1967.
- Which venues in England should display the official NHS QR code poster? *NHS*, citováno k 13. 6. 2022. Dostupné z: https://faq.covid19.nhs.uk/article/KA-01183/en-us?parentid=CAT-01043&rootid=CAT-01027
- WHITE, Lucie, Philippe VAN BASSHUYSEN. Without a trace: Why did corona apps fail? *Journal of Medical Ethics*, 2021, roč. 47, č. 12. Dostupné z: https://jme.bmj.com/content/47/12/e83
- WOODHAMS, Samuel. COVID-19 Digital Rights Tracker. *TOP10VPN*, publikováno 20. 3. 2020. Dostupné z: https://www.top10vpn.com/research/covid-19-digital-rights-tracker/
- YANG, Junwei, Timothy REUTER. 3 ways China is using drones to fight coronavirus. *World Economic Forum,* publikováno 16. 3. 2020. Dostupné z: https://www.weforum.org/agenda/2020/03/three-ways-china-is-using-drones-to-fight-coronavirus/

Autoři:
JUDr. MgA. Jakub Míšek, Ph.D.
Mgr. Anna Blechová
Mgr. Michael Bátrla
Mgr. Tereza Novotná
JUDr. Ladislav Vyhnánek, Ph.D., LL.M.
JUDr. Mgr. Jakub Harašta, Ph.D.
(všichni Masarykova univerzita, Právnická fakulta)

Masarykova univerzita
Žerotínovo nám. 617/9, 601 77 Brno

1. Vydání
Brno 2022