VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

Policejní a nemocniční databáze: přístupy k ochraně citlivých osobních údajů

Autor práce: Filip Hoza, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: Mgr. Michaela Brauneisová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Filip Hoza
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Policejní a nemocniční databáze: přístupy k ochraně citlivých osobních údajů
Název bakalářské práce v anglickém jazyce: Police and Hospital Databases: Approaches to the Protection of Sensitive Personal Data

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: Mgr. Michaela Brauneisová
Datum zadání bakalářské práce (měsíc, rok): prosinec 2025

Cíl bakalářské práce:

Hlavním cílem bakalářské práce je porovnat přístupy k nakládání a ochraně citlivých osobních údajů v policejních a nemocničních databázích, zhodnotit jejich silné a slabé stránky a identifikovat bezpečnostní postupy, které mohou být vzájemně inspirativní pro zvýšení úrovně ochrany dat v obou systémech.

Vedlejším cílem práce je zhodnotit právní úpravu nakládání s citlivými osobními údaji v policejních a nemocničních databázích, zmapovat zkušenosti jejich uživatelů a vyhodnotit silné i slabé stránky současné praxe s ohledem na možnosti zvýšení bezpečnosti a efektivity těchto databází.

Student: Filip Hoza, DiS.	5.12.2025 *datum*	*podpis*
Vedoucí práce: Mgr. Michaela Brauneisová	5.12.2025 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	9.1.2026 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	14.1.2026 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	15.1.2026 *datum*	*podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z.ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce Mgr. Michaele Brauneisové za cenné rady, připomínky a metodické vedení práce, celé své rodině za podporu a policistům sloužícím na OOP Cheb, kteří mi byli oporou při zpracování bakalářské práce.

ABSTRAKT

HOZA, F. *Policejní a nemocniční databáze: přístupy k ochraně citlivých osobních údajů.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 90 s. Vedoucí bakalářské práce: Mgr. Michaela Brauneisová

Klíčová slova: citlivé osobní údaje, ochrana osobních údajů, policejní databáze, nemocniční databáze, informační bezpečnost, právní úprava, databázové systémy

Bakalářská práce se zabývá ochranou citlivých osobních údajů v policejních a nemocničních databázích. Zaměřuje se na porovnání přístupů k nakládání a ochraně těchto údajů ve dvou odlišných typech databázových systémů, které se liší svým účelem, právním rámcem i okruhem oprávněných uživatelů. Hlavním cílem práce je porovnat přístupy k nakládání a ochraně citlivých osobních údajů v policejních a nemocničních databázích, zhodnotit jejich silné a slabé stránky a identifikovat bezpečnostní postupy, které mohou být vzájemně inspirativní pro zvýšení úrovně ochrany dat v obou systémech. Vedlejším cílem práce je zhodnotit právní úpravu nakládání s citlivými osobními údaji v policejních a nemocničních databázích, zmapovat zkušenosti jejich uživatelů a vyhodnotit silné i slabé stránky současné praxe s ohledem na možnosti zvýšení bezpečnosti a efektivity těchto databází. Teoretická část práce vychází z metod deskripce, komparace a studia odborné literatury a právních předpisů. Praktická část je založena na kvantitativním dotazníkovém šetření mezi uživateli obou databázových systémů. Výsledkem práce je zhodnocení současného stavu ochrany citlivých osobních údajů v policejních a nemocničních databázích a formulace návrhů opatření směřujících ke zvýšení bezpečnosti, efektivity a kvality nakládání s těmito údaji.

ABSTRACT

HOZA, F. *Police and Hospital Databases: Approaches to the Protection of Sensitive Personal Data.* České Budějovice: The College of European and Regional Studies, 2026. 90 p. Bachelor's thesis supervisor: Mgr. Michaela Brauneisová.

Key words: sensitive personal data, personal data protection, police databases, hospital databases, information security, legal regulation, database systems

This bachelor's thesis deals with the protection of sensitive personal data in police and hospital databases. It focuses on comparing approaches to the handling and protection of such data in two different types of database systems that differ in their purpose, legal framework, and the range of authorized users. The main aim of the thesis is to compare approaches to the handling and protection of sensitive personal data in police and hospital databases, assess their strengths and weaknesses, and identify security procedures that may serve as mutual inspiration for improving the level of data protection in both systems. The secondary aim is to evaluate the legal regulation of the handling of sensitive personal data in police and hospital databases, map the experience of their users, and assess the strengths and weaknesses of current practice with regard to the possibilities of increasing the security and efficiency of these databases. The theoretical part of the thesis is based on the methods of description, comparison, and the study of professional literature and legal regulations. The practical part is based on a quantitative questionnaire survey conducted among users of both database systems. The outcome of the thesis is an evaluation of the current state of protection of sensitive personal data in police and hospital databases and the formulation of proposals aimed at increasing the security, efficiency, and quality of the handling of such data.

Obsah

Úvod

Ochrana osobních údajů je v současné době velmi důležitým tématem, a to nejen z právního hlediska, ale i z hlediska každodenní praxe institucí, které s těmito údaji pracují. Zvláštní význam mají citlivé osobní údaje, protože jejich zneužití nebo neoprávněné zpřístupnění může výrazně zasáhnout do soukromí člověka a narušit důvěru ve fungování veřejných institucí. Mezi oblasti, ve kterých se s těmito údaji pracuje ve velkém rozsahu, patří zejména bezpečnostní složky a zdravotnická zařízení.

Policejní a nemocniční databáze představují dva odlišné systémy, které spojuje práce s velmi citlivými informacemi o fyzických osobách. Každý z těchto systémů však slouží jinému účelu a funguje v jiném právním i organizačním prostředí. Policejní databáze jsou využívány především při plnění úkolů v oblasti bezpečnosti, prevence a odhalování protiprávní činnosti, zatímco nemocniční databáze slouží zejména pro poskytování zdravotních služeb, vedení zdravotnické dokumentace a zajištění návaznosti péče o pacienta. Přestože jsou účely těchto databází rozdílné, v obou případech je nezbytné zajistit vysokou úroveň ochrany uchovávaných údajů. Právě porovnání těchto dvou oblastí může ukázat, v čem se jejich přístupy shodují, v čem se liší a jaké postupy by mohly být využitelné i v druhém prostředí.

Téma této bakalářské práce je aktuální nejen z pohledu práva a bezpečnosti, ale i z pohledu společnosti jako celku. V době rostoucí digitalizace a stále širšího využívání informačních systémů je ochrana citlivých osobních údajů jedním ze základních předpokladů řádného fungování institucí i důvěry veřejnosti v jejich činnost. Součástí práce bude také zhodnocení zkušeností uživatelů obou typů databází a posouzení současné praxe z hlediska bezpečnosti, přístupnosti a efektivity. Na základě teoretických poznatků i výsledků praktické části budou následně formulovány závěry a doporučení, která by mohla přispět ke zkvalitnění ochrany citlivých osobních údajů v obou sledovaných oblastech. V návaznosti na uvedené zaměření práce je proto dále vymezen její cíl a metodický postup, prostřednictvím kterého bude zkoumaná problematika zpracována.

1 Cíl a metodika bakalářské práce

Cílem bakalářské práce je porovnat přístupy k nakládání a ochraně citlivých osobních údajů v policejních a nemocničních databázích, zhodnotit jejich silné a slabé stránky a poukázat na bezpečnostní postupy, které mohou být pro obě oblasti vzájemně inspirativní. Práce vychází z předpokladu, že policejní a nemocniční databáze představují dva specifické informační systémy, které slouží odlišným účelům, avšak v obou případech dochází ke zpracování vysoce citlivých osobních údajů, jejichž ochrana musí odpovídat právním požadavkům i potřebám konkrétního prostředí.

Práce se dále zaměřuje na posouzení právní úpravy vztahující se k nakládání s citlivými osobními údaji v obou typech databází a na zhodnocení současné praxe z hlediska bezpečnosti, přístupnosti a efektivity. Pozornost je věnována také tomu, jak jsou v policejním a nemocničním prostředí nastavena pravidla přístupu k údajům, jaká bezpečnostní opatření jsou využívána a jaká rizika jsou s provozem těchto databázových systémů spojena.

Při zpracování bakalářské práce budou využity zejména metody deskripce, analýzy, komparace a výzkumné sondy. Metoda deskripce bude použita k charakteristice policejních a nemocničních databázových systémů, jejich funkcí, účelu a způsobu nakládání s citlivými osobními údaji. Analýza odborné literatury a relevantních právních předpisů poslouží k vymezení základních pojmů, k objasnění právního rámce a k zachycení odborných východisek zkoumané problematiky. Komparativní metoda umožní porovnat oba typy databází z hlediska právního rámce, úrovně ochrany údajů, pravidel přístupu k informacím i používaných bezpečnostních opatření.

Součástí práce bude také výzkumná sonda realizovaná formou dotazníkového šetření mezi pracovníky Policie České republiky a pracovníky nemocničních zařízení. Jejím cílem bude doplnit teoretická východiska o praktický pohled na fungování ochrany citlivých osobních údajů v databázových systémech, zjistit zkušenosti respondentů s jejich používáním a zachytit, jaká rizika nebo problematické oblasti jsou v praxi vnímány jako nejvýznamnější.

Na základě propojení poznatků z odborných zdrojů, právních předpisů a výsledků výzkumné sondy budou formulovány závěry týkající se silných a slabých stránek obou

systémů a naznačeny možnosti dalšího zlepšení ochrany citlivých osobních údajů v policejním i nemocničním prostředí.

2 Rozlišení základních pojmů

Pro potřeby této bakalářské práce je nejprve vhodné vymezit základní pojmy, se kterými bude dále pracováno. Téma je zaměřeno na policejní a nemocniční databáze a na ochranu citlivých osobních údajů, proto je třeba objasnit zejména pojmy data, informace, databáze, databázový systém, osobní údaje, citlivé osobní údaje a zpracování osobních údajů. Přesné rozlišení těchto pojmů je důležité nejen z odborného a právního hlediska, ale i pro správné pochopení dalších částí práce.

Vymezení základních pojmů má význam také proto, že v běžném jazyce bývají některé z nich používány nepřesně nebo zaměnitelně. Typicky dochází k zaměňování pojmů data a informace nebo databáze a databázový systém. Tato kapitola proto vytváří pojmový základ pro další výklad.

2.1 Data a informace

Pojem data lze chápat jako jednotlivé údaje, znaky, symboly nebo hodnoty, které samy o sobě ještě nemusejí mít jednoznačný vypovídací význam. Mohou mít podobu čísel, textových údajů, kódů, záznamů nebo jiných evidovaných skutečností. Data představují základní vstupy, se kterými je dále pracováno, tříděno je, ukládáno a následně vyhodnocováno. V odborném výkladu jsou data chápána jako statické hodnoty, které je třeba uchovat a dále zpracovávat.[1] V prostředí policejních a nemocničních databází mohou být daty například jméno a příjmení osoby, datum narození, rodné číslo, adresa bydliště, identifikační číslo pojištěnce, záznam o zdravotním vyšetření, údaj o hospitalizaci, informace o zákroku, záznam o policejním úkonu nebo například čas a místo určité události. Každý takový údaj může být sám o sobě izolovaný, avšak ve spojení s dalšími údaji získává širší význam.

Informace vzniká tehdy, když jsou jednotlivá data uspořádána, vzájemně propojena, vyhodnocena a zasazena do určitého kontextu. Jinými slovy lze říci, že informace je významově využitelný výstup z dat. Samotné datum narození je pouze datem, ale ve spojení se jménem a dalšími identifikačními údaji již vytváří informaci vztahující se ke konkrétní osobě. Obdobně samotný údaj o přijetí pacienta do nemocnice

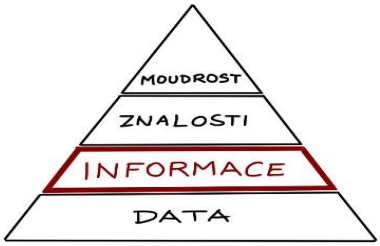
[1] KUTÍNOVÁ, Miluše a Jiří MACUR. *Informační technologie a systémová analýza: studijní opory pro studijní programy s kombinovanou formou studia* [online]. Brno: Vysoké učení technické v Brně, 2006, s. 20 [cit. 26. 3. 2026]. Dostupné z WWW: https://www.fce.vutbr.cz/aiu/macur.j/bu04/BU04_M01.pdf.

představuje jednotlivé datum, ale v souvislosti s diagnózou, průběhem léčby a výsledky vyšetření se stává součástí širší informace o zdravotním stavu pacienta.

Rozdíl mezi daty a informacemi je významný i z pohledu praktického fungování databází. Databáze neslouží pouze k mechanickému ukládání jednotlivých údajů, ale především k jejich organizaci a využití. To znamená, že údaje uložené v databázi mohou být vyhledávány, porovnávány, seskupovány a vyhodnocovány tak, aby poskytovaly informace důležité pro rozhodování nebo výkon konkrétní činnosti. V policejním prostředí mohou takto zpracovaná data sloužit například k identifikaci osoby nebo k objasňování určité události, ve zdravotnickém prostředí pak například k poskytování péče, sledování vývoje zdravotního stavu nebo návaznosti léčby. Rozlišení mezi daty a informacemi je podstatné také z hlediska ochrany osobních údajů. Ochrana se nevztahuje pouze na izolované údaje, ale na všechny informace, které lze spojit s určitou fyzickou osobou. V databázových systémech se proto často nechrání jen jednotlivé položky, ale celý soubor vzájemně propojených údajů, které ve svém celku vypovídají o identitě, zdravotním stavu, chování nebo právním postavení konkrétní osoby.

Tento vztah lze znázornit také pomocí pyramidy znalostí, v níž data tvoří základnu, z jejich uspořádání vznikají informace, jejich hlubším pochopením a interpretací pak znalosti a jejich nejvyšším stupněm je moudrost, tedy schopnost správně posoudit význam a důsledky získaných poznatků. V kontextu ochrany osobních údajů je podstatné, že riziko pro soukromí nevzniká pouze shromážděním jednotlivých dat, ale zejména jejich propojením do informací, následným vyhodnocením do znalostí a případným využitím těchto poznatků způsobem, který může významně zasáhnout do práv a soukromí konkrétní fyzické osoby.

Obrázek 1: Pyramida znalostí



Zdroj: www.ardit.cz

2.2 Databáze a databázový systém

V současné době jsou životy lidí stále více propojeny s digitálním prostředím, ve kterém hraje zpracování, uchovávání a sdílení informací zásadní roli. Moderní společnost je závislá na rychlém přístupu k datům a na možnosti tato data efektivně spravovat, vyhodnocovat a bezpečně ukládat. Databáze a databázové systémy proto představují jeden ze základních pilířů fungování celé řady oblastí lidské činnosti. Uplatnění nacházejí nejen v podnikání a veřejné správě, ale také ve vědě, bezpečnostních složkách, zdravotnictví, školství, dopravě, bankovnictví nebo v každodenním provozu institucí a organizací.

Pro účely této práce je vhodné odlišit pojem databáze od pojmu databázový systém. Zatímco databáze představuje uspořádaný soubor údajů, databázový systém zahrnuje také nástroje a programy umožňující s těmito údaji pracovat. Databázový systém je v odborné literatuře vymezován jako soubor vzájemně souvisejících dat a programů umožňujících přístup k těmto datům.[2]

Databáze lze obecně charakterizovat jako strukturované soubory dat, které jsou organizovány tak, aby umožňovaly jejich efektivní ukládání, vyhledávání, třídění, aktualizaci a následné využití. Smyslem databáze není pouze uchovávání velkého množství údajů, ale především jejich přehledné uspořádání a možnost rychlé práce s nimi. Odborná literatura současně upozorňuje, že databáze lze třídit z více hledisek, například podle obsahu, modelu ukládání dat, architektury nebo způsobu zpřístupnění uživatelům.[3] V běžném pojetí jsou data často ukládána do tabulek, v nichž každý řádek představuje konkrétní záznam a každý sloupec určitý typ údaje. Taková struktura umožňuje snadnější orientaci v uložených informacích a jejich vzájemné propojení.

Databázový systém představuje širší celek než samotná databáze. Zahrnuje nejen uložená data, ale také programové a technické prostředky, které umožňují jejich správu, vyhledávání, úpravu, zabezpečení a kontrolu přístupových oprávnění. Součástí databázového systému bývají rovněž mechanismy pro zálohování dat, obnovu po výpadku a správu více uživatelů současně. Tyto systémy lze rozdělit do několika

[2] SILBERSCHATZ, Avi; KORTH, Henry F.; SUDARSHAN, S. *Database System Concepts*. 7th ed. New York: McGraw-Hill, 2019, s. 1. ISBN 978-00-7802-215-9.

[3] CONNELLY KOHUTOVÁ, Radka. Databáze ve věku informační společnosti a jejich právní ochrana. Praha: C. H. Beck, 2013, s. 16. ISBN 978-80-7400-493-3.

základních skupin podle toho, jakým způsobem jsou v nich data organizována, ukládána a zpracovávána. Mezi nejvýznamnější typy databázových systémů patří relační, NoSQL, distribuované, in-memory a cloudové databázové systémy.

Vývoj databázových systémů prošel v průběhu času výraznou proměnou. Původně šlo spíše o jednodušší nástroje určené k ukládání a základní evidenci dat, zatímco dnes představují komplexní platformy schopné obsluhovat rozsáhlé informační systémy a pracovat s obrovským množstvím údajů v reálném čase. Současné databázové systémy musí vedle samotného ukládání dat zvládat také jejich sdílení mezi více uživateli, zajištění integrity a konzistence dat, ochranu před neoprávněným přístupem a zachování dostupnosti údajů i při vysokém zatížení systému. Právě z tohoto důvodu se databázové systémy staly zásadní součástí fungování institucí, které pracují s rozsáhlými databázemi, včetně policejních a nemocničních zařízení.

2.2.1 Relační databázové systémy

Relační databázové systémy, často označované zkratkou RDBMS, patří mezi nejrozšířenější a nejčastěji využívané typy databázových systémů. Jejich základním principem je ukládání dat do tabulek, mezi nimiž existují určité vztahy. Jednotlivé tabulky obsahují záznamy a tyto záznamy lze vzájemně propojovat prostřednictvím definovaných klíčů. Tím je umožněno vytvářet logicky uspořádané databázové struktury, které jsou přehledné a dobře spravovatelné.

Výhodou relačních databázových systémů je zejména přesně daná struktura dat, která přispívá k jejich přehlednosti, snadnějšímu vyhledávání a spolehlivější správě. Tyto systémy obvykle využívají dotazovací jazyk SQL, tedy Structured Query Language, jehož prostřednictvím lze data vkládat, upravovat, mazat i vyhledávat.

Relační databázové systémy se často používají v prostředích, kde je důležitá přesnost, konzistence a spolehlivost dat. Typické je jejich využití v bankovnictví, účetnictví, státní správě, nemocničních informačních systémech nebo v podnicích, kde je potřeba pracovat s přesně strukturovanými informacemi. Výhodou těchto systémů je rovněž možnost nastavení různých přístupových práv a kontrolních mechanismů, což je významné zejména tam, kde se pracuje s citlivými údaji. Mezi nejznámější relační databázové systémy patří Oracle Database, MySQL, Microsoft SQL Server a PostgreSQL.

2.2.2 NoSQL databázové systémy

NoSQL databázové systémy představují odlišný přístup k ukládání a správě dat než databáze relační. Na rozdíl od nich nevyužívají klasickou tabulkovou strukturu s pevně definovanými vztahy, ale jsou navrženy tak, aby dokázaly pracovat i s nestrukturovanými nebo polostrukturovanými daty. To znamená, že umožňují větší flexibilitu při ukládání údajů a lépe se přizpůsobují situacím, kdy se struktura dat často mění nebo kdy není předem přesně stanovena.

Tyto systémy vznikly především jako reakce na potřebu efektivně ukládat a zpracovávat velmi velké objemy dat, které by bylo v klasických relačních databázích obtížné spravovat. NoSQL databáze se proto uplatňují především v prostředí moderních webových aplikací, sociálních sítí, analytických systémů nebo služeb, které musí zpracovávat velké množství různorodých dat v krátkém čase. Jejich výhodou bývá vysoká škálovatelnost, rychlost a schopnost pracovat v distribuovaném prostředí.

NoSQL databáze mohou mít různé podoby. Některé fungují jako dokumentové databáze, jiné jako databáze klíč–hodnota, sloupcové databáze nebo grafové databáze. Každý z těchto přístupů je vhodný pro jiný typ využití. Dokumentové databáze například umožňují ukládat komplexnější datové struktury, zatímco databáze klíč–hodnota jsou vhodné tam, kde je požadována velmi rychlá práce s jednoduššími daty. Mezi známé příklady NoSQL databází patří MongoDB, Cassandra, Couchbase a Redis.

2.2.3 Distribuované databázové systémy

Distribuované databázové systémy umožňují ukládání a správu dat na více fyzických serverech nebo uzlech, které mohou být umístěny na různých místech. Na rozdíl od centralizovaných systémů, kde jsou data uložena na jednom místě, distribuované databáze rozdělují data mezi více zařízení, která spolu vzájemně komunikují. Tento princip přináší řadu výhod, zejména vyšší dostupnost systému, lepší odolnost vůči výpadkům a možnost efektivněji zpracovávat velké množství dat.

Jednou z hlavních předností distribuovaných databázových systémů je skutečnost, že data mohou být replikována na více místech. To znamená, že pokud dojde k výpadku jednoho serveru, systém může i nadále fungovat prostřednictvím jiného uzlu. Takové řešení je velmi důležité zejména v prostředích, kde je nutné zajistit nepřetržitou dostupnost informací a minimalizovat riziko ztráty dat. Distribuované systémy se proto

uplatňují například ve velkých organizacích, globálních službách nebo tam, kde je potřeba rychle zpracovávat data z více různých míst současně.

Nevýhodou těchto systémů může být jejich větší technická složitost. Správa distribuované databáze vyžaduje důkladné nastavení komunikace mezi jednotlivými uzly, synchronizaci dat a řešení případných konfliktů mezi různými verzemi uložených údajů. Přesto jsou distribuované databázové systémy v současné době velmi významné, protože dokáží reagovat na rostoucí požadavky na dostupnost, výkon a odolnost informačních systémů. Mezi známé příklady distribuovaných databázových systémů patří Apache Hadoop, Amazon DynamoDB, Google Bigtable a Apache Cassandra.

2.2.4 In-memory databázové systémy

In-memory databázové systémy jsou specifické tím, že ukládají data přímo do operační paměti počítače, nikoli primárně na pevný disk nebo jiné trvalé úložiště. Díky tomu umožňují velmi rychlé zpracování dat a dosahují vysokého výkonu při práci s rozsáhlými datovými soubory. Přístup k datům uloženým v paměti je totiž výrazně rychlejší než přístup k datům uloženým na tradičních datových médiích.

Tento typ databázových systémů je využíván především tam, kde je potřeba velmi rychlá odezva a zpracování dat v reálném čase. Může jít například o analytické systémy, finanční aplikace, monitorovací nástroje nebo služby, které pracují s velkým množstvím požadavků během krátkého časového úseku. In-memory databáze jsou vhodné zejména v situacích, kdy je rozhodující rychlost vyhledávání, třídění a analýzy dat.

Na druhou stranu je nutné počítat s tím, že ukládání dat do operační paměti klade vyšší nároky na technické vybavení a na zabezpečení proti výpadkům. Pokud by nebyla data pravidelně ukládána i na trvalé úložiště, mohlo by při poruše dojít k jejich ztrátě. Proto bývají tyto systémy často doplněny o mechanismy zálohování a obnovy dat. Mezi známé příklady in-memory databází patří SAP HANA, Oracle TimesTen a Redis.

2.2.5 Cloudové databázové systémy

Cloudové databázové systémy představují moderní způsob ukládání a správy dat v prostředí, které je poskytováno externím poskytovatelem služeb. Namísto toho, aby si organizace budovala a spravovala vlastní databázovou infrastrukturu, využívá vzdálené servery a služby dostupné prostřednictvím internetu. Tato forma řešení přináší větší flexibilitu, snadnější škálovatelnost a často i nižší náklady na provoz a údržbu.

Jednou z hlavních výhod cloudových databázových systémů je možnost rychle přizpůsobit kapacitu systému aktuálním potřebám organizace. Pokud je třeba ukládat větší objem dat nebo obsloužit více uživatelů, lze kapacitu systému zpravidla jednoduše navýšit. Stejně tak odpadá část starostí spojených se správou hardwaru, aktualizacemi nebo technickou údržbou, protože tyto činnosti zajišťuje poskytovatel cloudové služby.

Cloudové databáze jsou v současnosti velmi oblíbené zejména u organizací, které potřebují pružně reagovat na změny, rychle zavádět nové služby nebo provozovat systémy dostupné z více míst současně. Uplatnění nacházejí jak v soukromém sektoru, tak ve veřejné správě, zdravotnictví i dalších oblastech. Současně však vyvolávají i určité otázky spojené s bezpečností dat, s kontrolou nad uloženými informacemi a s odpovědností za ochranu osobních údajů. Právě proto je při využívání cloudových databázových systémů nezbytné věnovat zvýšenou pozornost smluvním podmínkám, zabezpečení přenosu dat a nastavení přístupových oprávnění. Mezi oblíbené cloudové databáze patří Amazon RDS, Microsoft Azure SQL Database, Google Cloud SQL a MongoDB Atlas.

2.2.6 Databázové a informační systémy v procesech organizace

Databázové a informační systémy nelze chápat pouze jako technické prostředky určené k ukládání a vyhledávání údajů. V praxi jsou součástí širšího fungování organizace a podílejí se na zajištění jejích hlavních, podpůrných i řídicích procesů. Jejich význam tedy nespočívá jen v evidenci dat, ale také v tom, že umožňují koordinaci činností, podporují rozhodování a přispívají k efektivnějšímu fungování celé organizace.

Z procesního hlediska je důležité, že každá organizace vykonává soubor navazujících činností, které směřují k naplnění jejího účelu. Tyto činnosti lze chápat jako procesy, přičemž některé z nich tvoří jádro její činnosti, jiné mají podpůrný charakter a další slouží k řízení a kontrole. Informační systém do tohoto uspořádání vstupuje tím, že poskytuje potřebná data pro jednotlivé kroky procesu, propojuje dílčí činnosti a umožňuje jejich lepší návaznost. Díky tomu lze sledovat nejen samotný průběh činností, ale také jejich výsledky, vzájemné vazby a případná slabá místa.

Význam této skutečnosti spočívá i v tom, že kvalita informačního systému má přímý dopad na kvalitu fungování celé organizace. Pokud je systém nepřehledný, neaktuální nebo neodpovídá reálným potřebám uživatelů, může zpomalovat pracovní postupy, komplikovat rozhodování a zvyšovat riziko chyb. Naopak správně nastavený

systém umožňuje rychlejší tok informací, lepší přehled o probíhajících činnostech a účinnější kontrolu nad tím, jak jsou jednotlivé úkoly plněny. Databázový systém se tak stává nejen nástrojem evidence, ale i důležitým prvkem organizační efektivity.

Tento obecný pohled je důležitý i pro zaměření této bakalářské práce. Policejní a nemocniční databáze totiž také nepředstavují pouze soubor uložených údajů, ale jsou součástí širšího systému činností a rozhodovacích procesů. V obou případech slouží jako informační základ pro výkon konkrétních úkolů, pro koordinaci postupu jednotlivých pracovníků i pro kontrolu správnosti a návaznosti prováděných úkonů. Právě proto je vhodné vnímat databáze nejen jako technický prostředek, ale jako součást organizačního fungování instituce.[4]

2.2.7 Dokumentace, autenticita a uchovávání dat v databázových systémech

Pro správné fungování databázových systémů nestačí pouze samotné ukládání dat. Důležitou součástí práce s daty je také jejich dokumentace, protože právě ta umožňuje pochopit původ, strukturu, obsah a způsob využití jednotlivých údajů. Bez dostatečné dokumentace může být práce s databází nepřehledná a v delším časovém horizontu i obtížně použitelná. Dokumentace by proto měla obsahovat základní informace o datovém souboru, jeho vzniku, uspořádání a případných změnách, ke kterým v průběhu práce s daty docházelo.

Vedle dokumentace je důležitá také autenticita dat, tedy jistota, že údaje odpovídají původnímu obsahu a nebyly nepovoleně nebo nepřehledně měněny. V databázových systémech je proto vhodné sledovat jednotlivé verze datových souborů, zaznamenávat provedené úpravy a uchovávat přehled o tom, kdo a kdy změny provedl. Takový postup přispívá k větší důvěryhodnosti databáze a současně umožňuje zpětnou kontrolu práce s daty.

Významnou součástí správy databázových systémů je i dlouhodobé uchovávání dat. S tím souvisí pravidelné zálohování, vhodná volba datových formátů a zajištění ochrany proti ztrátě nebo poškození údajů. Při uchovávání dat je třeba počítat i s technickým vývojem, protože některé formáty nebo nosiče mohou časem zastarávat. Z tohoto důvodu je důležité dbát nejen na samotné uložení dat, ale i na jejich budoucí

[4] SODOMKA, Petr a Hana KLČOVÁ. *Informační systémy v podnikové praxi. 2. aktualizované a rozšířené vydání.* Brno: Computer Press, 2010, s. 43. ISBN 978-80-251-2878-7.

dostupnost, čitelnost a použitelnost. Dokumentace, autenticita a uchovávání dat tak společně tvoří důležitý základ spolehlivého fungování databázových systémů.[5]

2.3 Osobní údaje a citlivé osobní údaje

Za osobní údaje jsou považovány veškeré informace o identifikované nebo identifikovatelné fyzické osobě. Zjednodušeně lze říci, že osobním údajem je jakýkoli údaj, podle kterého lze konkrétní osobu určit přímo nebo nepřímo. Nemusí jít pouze o jméno a příjmení, ale například také o rodné číslo, datum narození, adresu, telefonní číslo, e-mail, lokalizační údaj, obrazový záznam nebo jiné znaky, které lze spojit s určitou osobou.

Identifikovatelnou fyzickou osobou je taková osoba, kterou je možné určit přímo, například podle jména, nebo nepřímo, například pomocí kombinace více údajů. To je důležité zejména v databázových systémech, protože i údaje, které samy o sobě nemusí jednoznačně identifikovat konkrétního člověka, mohou ve spojení s dalšími daty vést k jeho přesnému určení. Právě proto je v prostředí databází nutné chápat osobní údaje v širších souvislostech.

Vedle obecných osobních údajů existuje i zvláštní skupina údajů, které vyžadují zvýšenou úroveň ochrany. V běžné řeči se pro ně používá označení citlivé osobní údaje. Současná právní terminologie však hovoří především o zvláštních kategoriích osobních údajů. Do této skupiny patří například údaje o zdravotním stavu, genetické a biometrické údaje, údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském vyznání, členství v odborech nebo údaje týkající se sexuálního života a sexuální orientace.

Pro potřeby této bakalářské práce bude pojem citlivé osobní údaje používán jako obecně srozumitelné označení pro údaje, které svou povahou vyžadují zvýšenou ochranu. Je tomu tak zejména proto, že jejich zneužití nebo neoprávněné zpřístupnění může vést k velmi závažnému zásahu do soukromí člověka. Tyto údaje mohou vypovídat o zdravotním stavu, osobním životě, sociální situaci nebo jiných skutečnostech, které jsou mimořádně intimní a které by neměly být bezdůvodně přístupné dalším osobám.

[5] KREJČÍ, Jindřich; LEONTIYEVA, Yana, eds. *Cesty k datům: zdroje a management sociálněvědních dat v České republice.* Praha: Sociologické nakladatelství (SLON), 2012. s. 65. ISBN 978-80-7419-111-4.

V nemocničním prostředí patří mezi citlivé osobní údaje zejména údaje o zdravotním stavu pacienta, jeho diagnózách, výsledcích vyšetření, léčbě, medikaci, zdravotnické dokumentaci nebo případných omezeních. V policejním prostředí mohou mít citlivý charakter například údaje související s trestní minulostí osoby, s průběhem prověřování, s vedeným řízením nebo s jinými bezpečnostně významnými okolnostmi. I když se charakter těchto údajů v obou prostředích liší, v obou případech jde o informace, jejichž ochrana má zásadní význam.

2.4 Zpracování osobních údajů

Zpracováním osobních údajů se rozumí jakákoli operace nebo soubor operací, které jsou s osobními údaji prováděny. Jedná se například o jejich shromažďování, zaznamenávání, ukládání, třídění, uspořádání, uchovávání, úpravu, vyhledávání, používání, zpřístupňování, předávání, omezení nebo výmaz. Tento pojem je tedy velmi široký a zahrnuje v podstatě celý životní cyklus osobních údajů.

Je důležité zdůraznit, že zpracování osobních údajů nezačíná až okamžikem jejich aktivního použití, ale již samotným získáním a zaevidováním údajů. Stejně tak nekončí pouze jejich využitím, ale zahrnuje i jejich uchovávání, kontrolu, případné sdílení a následné odstranění. V prostředí databázových systémů probíhá zpracování údajů prakticky nepřetržitě, protože údaje jsou do systému vkládány, aktualizovány, vyhledávány i dále používány v rámci konkrétních pracovních postupů.

Zpracování osobních údajů však nepředstavuje pouze technickou činnost, ale i činnost právně regulovanou. Každé zpracování musí mít určitý zákonný důvod, musí sledovat konkrétní účel a musí být omezeno na nezbytný rozsah. Údaje nemohou být zpracovávány bezdůvodně, svévolně nebo v rozsahu, který není potřebný pro naplnění daného účelu. Právě tato zásada je velmi důležitá zejména tam, kde se pracuje s citlivými údaji.

V policejním a nemocničním prostředí může být účel zpracování odlišný. V nemocničních databázích je zpracování údajů nezbytné zejména pro poskytování zdravotních služeb, vedení zdravotnické dokumentace a zajištění návaznosti péče o pacienta. V policejních databázích je účelem zpracování plnění úkolů v oblasti bezpečnosti, prevence, odhalování a objasňování protiprávní činnosti nebo plnění dalších zákonem stanovených úkolů. Právě rozdílnost účelu má významný vliv na rozsah zpracovávaných údajů i na nastavení pravidel jejich ochrany.

Se zpracováním údajů úzce souvisí i základní zásady, které mají být při nakládání s osobními údaji respektovány. Patří mezi ně zejména zákonnost, účelové omezení, minimalizace údajů, přesnost, omezení doby uchování a zabezpečení údajů. Tyto zásady představují základní rámec, podle kterého by mělo být zpracování osobních údajů nastaveno v každém systému, ať již jde o oblast zdravotnictví nebo policejní praxe.

2.5 Správce, zpracovatel a subjekt údajů

Dalšími důležitými pojmy v oblasti ochrany osobních údajů jsou správce, zpracovatel a subjekt údajů. Tyto pojmy vymezují postavení jednotlivých osob nebo institucí při zpracování osobních údajů a mají zásadní význam pro určení odpovědnosti, rozsahu oprávnění i povinností při nakládání s údaji.

Správcem je subjekt, který určuje účely a prostředky zpracování osobních údajů. Jinými slovy jde o toho, kdo rozhoduje o tom, proč budou osobní údaje zpracovávány, v jakém rozsahu a jakým způsobem. Správcem může být orgán veřejné moci, zdravotnické zařízení, policejní orgán nebo jiný subjekt, který má pravomoc o zpracování rozhodovat. Správce současně odpovídá za to, aby zpracování osobních údajů probíhalo v souladu s právními předpisy a aby byla přijata odpovídající opatření k jejich ochraně.

Zpracovatelem je naopak ten, kdo osobní údaje zpracovává pro správce a na základě jeho pokynů. Nejde tedy o subjekt, který sám stanoví účel zpracování, ale o osobu nebo instituci, která se na zpracování podílí z technického nebo organizačního hlediska. Zpracovatel může například zajišťovat provoz informačního systému, správu databáze nebo jiné činnosti související s uchováváním a zpracováním údajů. Přestože o účelu zpracování nerozhoduje, i na něj dopadají povinnosti spojené s ochranou osobních údajů.

Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují. V kontextu této bakalářské práce se může jednat například o pacienta zdravotnického zařízení, osobu evidovanou v policejní databázi, oznamovatele, poškozeného, svědka nebo jinou osobu, o níž jsou v daném systému vedeny údaje. Právě subjekt údajů je tím, jehož soukromí a práva mají být prostřednictvím právní úpravy ochrany osobních údajů chráněny.

S postavením subjektu údajů úzce souvisí také jeho práva při zpracování osobních údajů. Subjekt údajů není pouze osobou, které se údaje týkají, ale také nositelem práv, jejichž účelem je posílit jeho kontrolu nad tím, jak je s jeho osobními údaji nakládáno. Mezi základní práva patří zejména právo na přístup k osobním údajům, právo na opravu

nebo doplnění nepřesných či neúplných údajů a za splnění zákonných podmínek také právo na výmaz osobních údajů.[6]

Právo na přístup umožňuje subjektu údajů zjistit, zda jsou jeho osobní údaje zpracovávány, v jakém rozsahu, za jakým účelem a případně komu mohou být zpřístupněny. Právo na opravu a doplnění směřuje k tomu, aby byly o subjektu údajů vedeny údaje správné, přesné a aktuální. Pokud jsou zpracovávané údaje nepřesné nebo neúplné, může subjekt údajů požadovat jejich opravu nebo doplnění. Právo na výmaz pak nelze chápat jako právo absolutní, protože jeho uplatnění vždy závisí na konkrétním právním důvodu zpracování a na tom, zda neexistuje jiný zákonný důvod pro další uchování údajů.

Rozlišení rolí správce, zpracovatele a subjektu údajů je důležité zejména proto, že umožňuje určit, kdo odpovídá za zákonnost zpracování, kdo přijímá bezpečnostní opatření, kdo zajišťuje technický provoz systému a komu náleží práva spojená s ochranou osobních údajů. Bez tohoto pojmového rozlišení by nebylo možné přesně určit odpovědnost jednotlivých subjektů ani správně posoudit jejich postavení při nakládání s osobními údaji v praxi.

2.6 Zabezpečení údajů a přístupová oprávnění

V souvislosti s databázovými systémy je nezbytné vymezit také pojmy zabezpečení údajů a přístupová oprávnění. Tyto pojmy mají v prostředí policejních i nemocničních databází zásadní význam, protože právě jejich správné nastavení rozhoduje o tom, zda budou uložené údaje skutečně chráněny před neoprávněným zásahem.

Zabezpečením údajů se rozumí soubor technických, organizačních a personálních opatření, jejichž cílem je chránit údaje před neoprávněným přístupem, ztrátou, poškozením, změnou, únikem nebo zneužitím. Nejde tedy pouze o jednorázové technické opatření, ale o širší systém ochrany, který zahrnuje více vzájemně propojených prvků. K zabezpečení údajů patří například ochrana přístupových hesel, ověřování identity uživatelů, evidence přístupů, omezení oprávnění, zálohování dat, kontrolní mechanismy nebo zabezpečení informační infrastruktury.

[6] JANEČKOVÁ, Eva. GDPR. *Praktická příručka implementace*. Praha: Wolters Kluwer ČR, 2018. s. 23. ISBN 978-80-7552-248-1.

Význam zabezpečení údajů je zvlášť výrazný v případech, kdy databáze obsahují vysoce citlivé údaje. V takové situaci nestačí pouze formálně upravit pravidla přístupu, ale je nutné vytvořit takové podmínky, aby k údajům skutečně měly přístup jen oprávněné osoby a aby bylo možné dohledat, kdo, kdy a za jakým účelem s údaji pracoval. Zabezpečení údajů proto zahrnuje nejen prevenci, ale i kontrolu a zpětnou dohledatelnost jednotlivých úkonů.

Přístupová oprávnění představují pravidla určující, kdo může s konkrétními údaji pracovat a v jakém rozsahu. Ne každá osoba, která je součástí určité instituce, musí mít přístup ke všem údajům uloženým v systému. Rozsah oprávnění by měl odpovídat pracovnímu zařazení, konkrétní činnosti a nezbytné potřebě přístupu k údajům. Tento princip je důležitý zejména v prostředí, kde je s citlivými údaji pracováno ve velkém rozsahu a kde by plošný přístup představoval výrazné bezpečnostní riziko.

V nemocničním prostředí může být přístup k údajům rozdělen podle profesního zařazení jednotlivých pracovníků, například mezi lékaře, zdravotní sestry, administrativní pracovníky nebo technickou podporu. V policejním prostředí může být přístup k údajům omezen podle typu útvaru, druhu činnosti, služebního zařazení nebo konkrétního oprávnění vyplývajícího z pracovního úkolu. V obou případech platí, že čím citlivější údaje systém obsahuje, tím důsledněji musí být nastavena pravidla přístupu.

Důležitou roli zde hraje i lidský faktor. Sebelepší technické zabezpečení nemusí být dostatečné, pokud osoby pracující se systémem nedodržují pravidla, podceňují význam ochrany údajů nebo jednají nedbale. Ochrana údajů proto nespočívá pouze v technickém nastavení systému, ale i v odpovědném přístupu uživatelů, v jejich poučení a v dodržování vnitřních pravidel dané instituce.

3 Policejní databáze

Policejní databáze představují významnou součást činnosti Policie České republiky. V podmínkách moderní společnosti, která je stále více závislá na rychlém přístupu k informacím a jejich efektivním zpracování, mají databázové systémy zásadní význam pro plnění úkolů v oblasti bezpečnosti, prevence a odhalování protiprávní činnosti. Nejde přitom pouze o technické nástroje určené k ukládání údajů, ale o informační prostředí, které umožňuje jejich shromažďování, evidenci, vyhledávání, propojení a vyhodnocování pro potřeby policejní praxe.

Význam policejních databází spočívá zejména v tom, že umožňují pracovat s velkým množstvím údajů rychle, systematicky a přehledně. V policejní praxi je nezbytné mít k dispozici informace o osobách, vozidlech, událostech, hledaných či pohřešovaných osobách, odcizených věcech nebo dalších skutečnostech důležitých pro zajištění veřejného pořádku a bezpečnosti. Databázové systémy tak policii usnadňují orientaci v rozsáhlém množství údajů a přispívají k efektivnějšímu výkonu jejích zákonných oprávnění.

Současně je však třeba zdůraznit, že policejní databáze pracují s údaji, které mohou mít osobní, a v některých případech i citlivý charakter. Z tohoto důvodu je jejich fungování neoddělitelně spojeno s právní úpravou zpracování osobních údajů, s pravidly přístupu k informacím a s požadavkem na odpovídající zabezpečení. Policejní databáze proto nelze chápat pouze jako prostředek evidence a správy dat, ale také jako oblast, v níž je nezbytné vyvažovat zájem na ochraně společnosti se zájmem na ochraně soukromí a práv jednotlivce.

Tato kapitola se zaměřuje na vymezení policejních databází, jejich účel a význam, právní rámec jejich fungování, typy zpracovávaných údajů a vybrané evidence využívané v policejním prostředí. Pozornost bude věnována také ochraně osobních údajů, nakládání s citlivými osobními údaji, bezpečnostním opatřením a rizikům, která jsou se zpracováním údajů v policejních databázích spojena.

3.1 Pojem a vymezení policejních databází

Policejní databáze lze vymezit jako soubory evidovaných údajů, se kterými Policie České republiky pracuje při plnění svých úkolů. Slouží k tomu, aby bylo možné informace přehledně ukládat, vyhledávat, porovnávat a využívat v konkrétních situacích policejní praxe. Nejde tedy pouze o technické prostředky pro uchovávání dat,

ale o nástroj, který umožňuje účelnou práci s informacemi významnými pro činnost policie.

Pod pojem policejní databáze lze zahrnout jak evidence vedené přímo policií, tak i další informační zdroje, k nimž policie přistupuje na základě zákonného oprávnění. Policejní praxe je totiž založena na využívání více navazujících evidencí a na propojování informací z různých zdrojů v rozsahu odpovídajícím pravomocem policie.

Charakteristickým znakem policejních databází je jejich účelové zaměření. Nejsou vytvářeny za účelem obecného shromažďování informací, ale pro potřeby konkrétní policejní činnosti. Obsahují údaje vztahující se například k osobám, věcem, vozidlům, událostem nebo jiným skutečnostem důležitým pro zajišťování bezpečnosti, pátrání, objasňování protiprávního jednání a plnění dalších úkolů policie.

Současně je třeba zdůraznit, že policejní databáze pracují s údaji, které mohou zasahovat do soukromí fyzických i právnických osob. Z tohoto důvodu je nezbytné dbát na zákonnost jejich využívání, omezení přístupu a odpovídající ochranu zpracovávaných údajů.

3.2 Účel a význam policejních databází

Účel těchto databází vyplývá ze samotného poslání Policie České republiky. Policie podle zákona slouží veřejnosti, chrání bezpečnost osob a majetku a veřejný pořádek, předchází trestné činnosti a plní úkoly podle trestního řádu a dalších právních předpisů. Databázové systémy proto představují důležitý nástroj, který umožňuje tyto úkoly plnit efektivněji a systematičtěji.

Z veřejně dostupných informací Policie České republiky vyplývá, že osobní údaje jsou policií zpracovávány zejména za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky a udržování veřejného pořádku a vnitřní bezpečnosti. Tyto systémy tak neslouží pouze k evidenci údajů, ale také k jejich aktivnímu využití při konkrétní policejní činnosti.

Jejich význam spočívá především v tom, že umožňují rychlý přístup k relevantním informacím. V policejní praxi je často nezbytné bez zbytečného odkladu ověřit totožnost osoby, zjistit souvislosti s konkrétní událostí, prověřit pátrání po osobě nebo věci nebo vyhodnotit informace důležité pro další služební postup. Databáze tak přispívají

k rychlosti rozhodování, k lepší orientaci v dostupných údajích a k návaznosti jednotlivých policejních úkonů.

Současně mají význam preventivní, evidenční i analytický. Neslouží jen k řešení již vzniklých případů, ale také k odhalování souvislostí mezi jednotlivými jevy, ke sledování opakujících se okolností a k podpoře preventivních opatření. Vedle toho plní i funkci organizační a kontrolní, protože umožňují zachycovat průběh vybraných úkonů a vytvářejí podmínky pro kontrolu zákonnosti zpracování údajů.

Pro fungování policie mají proto zásadní význam. Umožňují efektivnější plnění zákonných úkolů, rychlejší práci s informacemi a lepší orientaci v údajích důležitých pro bezpečnostní a trestněprávní činnost. Současně však jejich význam roste úměrně s odpovědností za zákonné a bezpečné nakládání s údaji, které obsahují.

3.3 Právní rámec policejních databází

Právní rámec policejních databází je tvořen několika navzájem propojenými úrovněmi právní úpravy. Základní postavení v českém právním řádu má zákon č. 273/2008 Sb., o Policii České republiky, který upravuje postavení policie, její úkoly a oprávnění a současně obsahuje i zvláštní pravidla pro zpracování osobních údajů při plnění některých policejních úkolů. Významnou roli má také zákon č. 110/2019 Sb., o zpracování osobních údajů, jenž v českém právu upravuje jak obecné otázky ochrany osobních údajů, tak zvláštní režim pro příslušné orgány v oblasti prevence, vyhledávání, odhalování a stíhání trestné činnosti. Na evropské úrovni je pak rozhodující směrnice Evropského parlamentu a Rady (EU) 2016/680, která je určena právě pro zpracování osobních údajů příslušnými orgány pro trestněprávní a bezpečnostní účely.

Zákon o Policii České republiky je pro policejní databáze klíčový především proto, že vymezuje samotné úkoly policie a současně vytváří právní základ pro práci s informacemi potřebnými k jejich plnění. S právním rámcem policejních databází souvisí již prvotní získávání osobních údajů. V tomto směru je významné ustanovení § 63 zákona o Policii České republiky, které upravuje oprávnění policisty vyzvat osobu k prokázání totožnosti v zákonem vymezených případech. Podle § 63 odst. 1 se prokázáním totožnosti rozumí prokázání jména, popřípadě jmen, příjmení, data narození a v případě potřeby také adresy místa trvalého pobytu, adresy místa pobytu nebo adresy bydliště v zahraničí,

rodného čísla a státní příslušnosti.[7] I takto zjištěné identifikační údaje mohou následně vstupovat do policejního informačního zázemí a být dále využívány při plnění zákonných úkolů policie.

Vedle toho může policie za zákonem stanovených podmínek získávat i informace z dalších evidencí vedených jinými správci. Podle § 66 zákona o Policii České republiky může v rozsahu potřebném pro plnění konkrétního úkolu žádat údaje z celé řady registrů a evidencí, například z evidence obyvatel, rejstříku trestů, evidence přestupků, registru silničních vozidel nebo registru řidičů.[8] Tím je vytvořen zákonný základ pro to, aby policejní činnost byla informačně propojena i s dalšími veřejnými evidencemi.

Pro vlastní policejní databáze je však stěžejní především § 79 zákona o Policii České republiky a navazující ustanovení. Toto ustanovení stanoví, že zvláštní pravidla o zpracování osobních údajů se použijí na zpracování údajů za účelem předcházení, vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky a zajišťování veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech.[9] Zákon současně zdůrazňuje, že policie může osobní údaje zpracovávat pouze tehdy, je-li to pro uvedené účely nezbytné. Právní úprava tak staví na zásadě účelovosti a nezbytnosti zpracování. Zvláštní význam má rovněž § 79 odst. 3, podle něhož lze shromažďovat údaje o rasovém nebo etnickém původu, náboženském, filozofickém nebo politickém přesvědčení, členství v odborové organizaci, zdravotním stavu, sexuálním chování nebo sexuální orientaci pouze tehdy, je-li to nezbytné pro účely šetření konkrétního trestného činu nebo přestupku.[10] Zákon tím přímo stanoví přísnější režim pro nejcitlivější okruhy údajů. Současně ukládá, aby policie údaje zpracovávané pro trestněprávní a bezpečnostní účely vedla odděleně od údajů zpracovávaných při plnění jiných úkolů policie. Komentářová literatura k tomuto ustanovení upozorňuje, že jde o zvláštní právní režim policejního zpracování osobních údajů, který je třeba vykládat restriktivně a vždy ve vazbě na konkrétní zákonný účel plnění policejních úkolů. Zároveň zdůrazňuje, že policejní zpracování údajů se odlišuje od běžného obecného

[7] ČESKO. Zákon č. 273 ze dne 17. července 2008 o Policii České republiky. In: Sbírka zákonů, Česká republika. 2008, § 63 odst.1. Dostupné z WWW: https://mv.gov.cz/soubor/sb091-08-pdf.aspx. ISSN 1211-1244
[8] Tamtéž, § 66.
[9] Tamtéž, § 79
[10] Tamtéž, § 79 odst. 3

režimu ochrany osobních údajů tím, že sleduje specifické veřejnoprávní cíle související s bezpečností a trestněprávní oblastí.[11]

Další významnou součástí právního rámce je zákon č. 110/2019 Sb., o zpracování osobních údajů. Ten navazuje na evropskou úpravu a v českém právu rozlišuje obecný režim ochrany osobních údajů a zvláštní režim pro příslušné orgány. Pro policejní databáze je důležitá zejména část upravující zpracování osobních údajů pro účely prevence, vyhledávání, odhalování a stíhání trestné činnosti a další související bezpečnostní účely. Tento zákon současně upravuje i některá omezení práv subjektů údajů, například pokud jde o přístup k údajům, jejich opravu, výmaz nebo omezení zpracování, jestliže by plné uplatnění těchto práv mohlo ohrozit nebo zmařit účel zpracování.

Zákon o zpracování osobních údajů však neřeší pouze samotné oprávnění osobní údaje shromažďovat. Ukládá také povinnost přijímat odpovídající technická a organizační opatření k zajištění jejich ochrany a při automatizovaném zpracování vyžaduje vedení elektronických záznamů, z nichž bude možné zjistit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány. Pro policejní databáze to znamená, že právní rámec nevymezuje jen oprávnění údaje získávat a používat, ale současně stanoví požadavky na jejich zabezpečení, dohledatelnost práce s nimi a odpovědnost oprávněných osob.

Na evropské úrovni je pro policejní databáze rozhodující směrnice (EU) 2016/680. Ta byla přijata právě pro ochranu fyzických osob při zpracování osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů. Její význam spočívá zejména v tom, že potvrzuje zvláštnost policejního a trestněprávního zpracování údajů a odlišuje je od obecného režimu podle obecného nařízení o ochraně osobních údajů. Zákon č. 110/2019 Sb. na tuto směrnici výslovně navazuje a představuje její vnitrostátní provedení. Pro výklad policejních databází je proto nezbytné vnímat českou právní úpravu i v širším evropském kontextu.

Pro úplnost je vhodné dodat, že Policie České republiky na svých oficiálních stránkách sama rozlišuje zpracování osobních údajů pro trestněprávní účely a zpracování

[11] ŠTEINBACH, Miroslav; ŠLESINGER, René; ZIMMERMANN, Miroslav; BÍLEK, Milan; HLAVÁČKOVÁ, Kateřina. *Zákon o Policii České republiky: Komentář.* Praha: Wolters Kluwer ČR, 2019. s. 193. ISBN 978-80-7598-193-6.

podle obecného nařízení o ochraně osobních údajů. Uvádí přitom, že obecným právním titulem pro zpracování osobních údajů jsou zejména §§ 2, 60 a 79 zákona č. 273/2008 Sb., přičemž konkrétní právní titul může vyplývat i z dalších zvláštních zákonných ustanovení. To potvrzuje, že právní rámec policejních databází není tvořen jediným předpisem, ale soustavou pravidel, která je třeba vždy posuzovat podle konkrétního účelu zpracování a povahy evidovaných údajů.

Pro úplnost je vhodné dodat, že zvláštní zákonná úprava zpracování osobních údajů se nevztahuje pouze na Policii České republiky, ale i na další bezpečnostní složky veřejné správy. Také zákon o obecní policii obsahuje samostatné ustanovení věnované zpracování osobních údajů obecní policií. Podle § 24a zákona č. 553/1991 Sb., o obecní policii, obecní policie zpracovává osobní údaje, které potřebuje k plnění úkolů podle tohoto nebo zvláštního zákona, a může je poskytovat policii, orgánům obce a dalším orgánům veřejné moci, je-li to nutné k plnění jejich úkolů. Současně zákon ukládá, aby obecní policie nejméně jednou za tři roky prověřovala, zda jsou takto zpracovávané osobní údaje nadále potřebné, a pokud tomu tak není, bez zbytečného odkladu provedla jejich likvidaci.[12]

Z uvedeného vyplývá, že právní rámec policejních databází je tvořen soustavou vzájemně propojených právních předpisů na národní i evropské úrovni. Stěžejní význam má zejména zákon č. 273/2008 Sb., o Policii České republiky, zákon č. 110/2019 Sb., o zpracování osobních údajů, a směrnice Evropského parlamentu a Rady (EU) 2016/680. Tyto předpisy společně upravují podmínky zákonného shromažďování, ukládání, využívání, předávání i kontroly osobních údajů v policejním prostředí a současně vymezují meze, které mají chránit práva a svobody dotčených osob.

3.4 Typologie údajů zpracovávaných v policejních databázích

Policejní databáze nepracují s jedním jednotným okruhem informací, ale s více skupinami údajů, které se liší svým obsahem, účelem i mírou citlivosti. Základní členění lze provést podle toho, zda jde o údaje identifikační, údaje o věcech a vozidlech, údaje o událostech a řízeních, údaje analytické a geografické nebo o údaje zvláštních kategorií, jejichž zpracování podléhá přísnějším podmínkám.

[12] ŠEBESTA, Patrik. *Zákon o obecní policii: Komentář.* Praha: Wolters Kluwer ČR, 2018. s. 241. ISBN 978-80-7552-455-3.

První a nejzákladnější skupinu tvoří identifikační a osobní údaje. Patří sem zejména jméno a příjmení, datum narození, adresa, rodné číslo nebo jiné identifikátory, které umožňují určit konkrétní osobu. V policejním prostředí se k nim mohou připojovat i další evidenční údaje, například informace o procesním postavení osoby, o jejím vztahu ke konkrétní události nebo o předchozích relevantních úkonech.

Další významnou skupinu představují biometrické a genetické údaje. V českém policejním prostředí jde zejména o daktyloskopické údaje, fotografie, případně biologické vzorky a z nich odvozené deoxyribonukleové profily. Tyto údaje mají zvláštní povahu, protože umožňují velmi přesnou identifikaci osoby a současně výrazně zasahují do soukromí, a proto podléhají přísnějšímu právnímu režimu.

Samostatnou skupinu tvoří údaje o vozidlech a dalších předmětech zájmu. Policie pracuje například s registračními značkami, údaji o vlastnictví a provozu vozidla, informacemi o odcizení vozidla nebo o jeho účasti na dopravní nehodě. Vedle toho eviduje i údaje o odcizených předmětech, zbraních, střelivu, drogách, zajištěných důkazech nebo jiných věcech významných pro trestní a správní řízení.

Velmi podstatnou skupinu představují údaje o incidentech, událostech a řízeních. Jde o záznamy o trestných činech, přestupcích, dopravních nehodách, bezpečnostních událostech nebo jednotlivých úkonech policie. Tyto údaje obsahují informace o čase, místě, způsobu spáchání, zúčastněných osobách, zajištěných věcech i procesním vývoji věci.

S touto kategorií úzce souvisí i záznamy, které policie pořizuje při plnění svých úkolů. Policejní právo připouští pořizování zvukových, obrazových nebo jiných záznamů, pokud je to nezbytné pro plnění zákonných úkolů policie. Takové záznamy pak nepředstavují pouze jednorázový dokumentační prostředek, ale mohou se stát součástí další evidenční, kontrolní nebo důkazní práce policie. Z hlediska typologie údajů je proto vhodné na ně nahlížet jako na specifickou podskupinu údajů o událostech a policejních úkonech, protože zachycují průběh konkrétní situace, jednání osob i okolnosti zásahu nebo šetření.[13]

Další skupinu tvoří analytická, statistická a geografická data. Nejde vždy o údaje, které by samy o sobě identifikovaly konkrétní osobu, ale často vznikají jako výstup

[13] HABICH, Lukáš; STEIN, Petr; HLAVÁČKOVÁ, Kateřina. *Policejní právo.* Praha: Wolters Kluwer ČR, 2025. s. 162–163. ISBN 978-80-7676-606-8.

z předchozího zpracování většího množství údajů. Může jít například o mapy kriminality, analýzy rizikových míst, prostorové rozložení trestné činnosti nebo souhrnné přehledy o bezpečnostní situaci.

Z hlediska právní ochrany je podstatné, že jednotlivé skupiny údajů nemají stejný režim. Zákon o Policii České republiky výslovně rozlišuje mezi běžnými osobními údaji a údaji o rasovém nebo etnickém původu, náboženském, filozofickém nebo politickém přesvědčení, členství v odborové organizaci, zdravotním stavu, sexuálním chování nebo sexuální orientaci. Tyto údaje lze shromažďovat pouze tehdy, je-li to nezbytné pro šetření konkrétního trestného činu nebo přestupku nebo při poskytování ochrany osob.

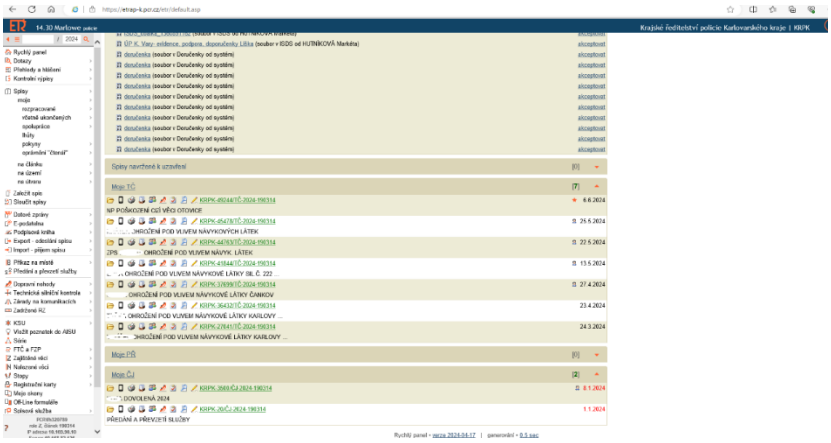
Policejní databáze tedy zahrnují několik navazujících kategorií údajů: osobní a identifikační údaje, biometrické a genetické údaje, údaje o vozidlech a věcech, údaje o incidentech a řízeních i údaje analytické a geografické. Právě tato mnoho různorodost vysvětluje, proč jsou policejní databáze významným, ale současně i citlivým nástrojem veřejné moci.

3.5 Vybrané policejní databáze a evidence

Policejní databáze netvoří jeden uzavřený celek, ale soustavu různých evidencí a informačních systémů, které se liší svým účelem, rozsahem zpracovávaných údajů i okruhem oprávněných uživatelů. Některé slouží především interním potřebám Policie České republiky, jiné mají částečně veřejný charakter a umožňují občanům nebo dalším subjektům vyhledávat konkrétní údaje v rozsahu stanoveném zákonem. Oficiální portál Policie ČR mezi databázemi uvádí například pátrání po osobách, pátrání po vozidlech, odcizené mobilní telefony, neplatné doklady, databázi PNR, databázi PSEUD, databázi UBYPORT, centrální registr zbraní, mapy kriminality nebo ztotožnění mrtvol. Už tento výčet ukazuje, že policejní databázové prostředí je velmi rozmanité a nelze je redukovat jen na klasické trestní evidence.

Z hlediska praktické policejní práce má významné postavení informační systém ETŘ, tedy Evidence trestního řízení. Z veřejně dostupných informací Policie ČR vyplývá, že jde o informační systém používaný v oblasti spisové služby a trestního řízení a že jeho provoz je upravován interními akty řízení policejního prezidenta. Pro tuto práci je důležité zejména to, že ETŘ ukazuje silné propojení policejní činnosti s digitální správou spisové a procesní agendy.

Obrázek 2: ETŘ



Zdroj: OOP Cheb - město

K veřejně nejznámějším databázím patří pátrání po osobách a pátrání po vozidlech. Tyto evidence umožňují zveřejnit údaje v rozsahu nezbytném k plnění úkolů policie, typicky při pátrání po hledaných nebo pohřešovaných osobách nebo po odcizených vozidlech. Jejich význam spočívá v tom, že propojují policejní činnost s veřejností a zvyšují šanci na získání poznatků vedoucích k nalezení osoby nebo věci. Současně však právě u těchto databází vystupuje otázka přiměřenosti zveřejnění osobních údajů, protože veřejná publikace údajů představuje intenzivnější zásah do soukromí než interní policejní evidence.

Další specifickou databází je PNR, tedy systém využívající údaje jmenné evidence cestujících. Policie na svých stránkách uvádí, že PNR data pocházejí z rezervačních a odbavovacích systémů leteckých dopravců a slouží ke sdílení údajů s národním útvarem pro informace o cestujících. Využití těchto údajů je spojováno zejména s prevencí, odhalováním, vyšetřováním a stíháním teroristických trestných činů a závažné trestné činnosti.

Zcela odlišný charakter má PSEUD, tedy Portál systému evidence uměleckých děl. Podle Policie ČR jde o specializovanou pátrací databázi odcizených, nalezených a navrácených předmětů kulturní hodnoty. Tato databáze ukazuje, že policejní informační systémy nemusí být zaměřeny jen na osoby nebo trestné činy, ale i na specifické oblasti veřejného zájmu.

Do policejního databázového prostředí patří také UBYPORT, což je webová aplikace určená k zasílání údajů o ubytovaných cizincích Policii České republiky v elektronické podobě. Jde o nástroj využívaný ubytovateli k plnění oznamovací

povinnosti prostřednictvím internetu. Tato evidence propojuje policejní činnost s externími subjekty a slouží zejména evidenčním a kontrolním účelům v oblasti pobytu cizinců.

Mimořádný význam má také Centrální registr zbraní. Z veřejných informací vyplývá, že slouží ke správě údajů o zbraních, střelivu a munici i o jejich držitelích a policie jej využívá k vydávání oprávnění i k analytické práci. Jde o databázi, která spojuje administrativní, kontrolní a bezpečnostní funkci.

Vedle toho Policie ČR zpřístupňuje i mapy kriminality, mapu varen a pěstíren nebo dopravní nehody v mapě. Tyto systémy ukazují posun od klasické textové evidence k vizualizaci a analytickému zpracování údajů. Jejich přínos spočívá zejména ve zpřehlednění bezpečnostní situace a v možnosti sledovat prostorové souvislosti kriminality či dopravní nehodovosti.

Vybrané policejní databáze a evidence ukazují šíři policejního informačního prostředí. Vedle interních systémů, jako je ETŘ, existují veřejně přístupné pátrací databáze, specializované systémy typu PSEUD nebo PNR a správní evidence, jakou je Centrální registr zbraní. Pro tuto práci je podstatné, že každá z těchto databází pracuje s jiným typem údajů, sleduje jiný účel a vyžaduje odlišný model ochrany. Právě tato rozrůzněnost vysvětluje, proč nelze otázku ochrany osobních údajů v policejním prostředí řešit jedním univerzálním přístupem.

3.6 Ochrana osobních údajů v policejním prostředí

Ochrana osobních údajů v policejním prostředí vychází z obecného ústavního a evropského požadavku chránit soukromí jednotlivce, současně však musí respektovat zvláštní povahu policejní činnosti. Policie nepracuje s osobními údaji nahodile nebo pro soukromé účely, ale při plnění zákonem vymezených úkolů v oblasti bezpečnosti, prevence a stíhání protiprávního jednání. Právě proto je policejní zpracování osobních údajů postaveno na zvláštním režimu, který je v českém právu vyjádřen zejména v zákoně o Policii České republiky a v zákoně o zpracování osobních údajů. Evropské právo přitom vychází z toho, že oblast prevence, vyšetřování, odhalování a stíhání trestných činů je upravena zvláštním právním aktem Unie, a nikoli pouze obecným režimem GDPR.

Základním pravidlem je zásada nezbytnosti a účelovosti. Podle zákona o Policii ČR může policie zpracovávat osobní údaje tehdy, je-li to nezbytné pro účely předcházení,

vyhledávání a odhalování trestné činnosti, stíhání trestných činů, zajišťování bezpečnosti České republiky nebo veřejného pořádku a vnitřní bezpečnosti, včetně pátrání po osobách a věcech. Současně zákon stanoví, že údaje zpracovávané pro tyto účely mají být vedeny odděleně od osobních údajů zpracovávaných při plnění jiných úkolů policie. Ochrana osobních údajů v policejním prostředí tedy nezačíná až technickým zabezpečením databází, ale už samotným zákonným vymezením důvodů a hranic jejich zpracování.

Důležitým prvkem ochrany je také institucionální odpovědnost. Zákon o Policii ČR počítá s pověřencem pro ochranu osobních údajů, kterého jmenuje policejní prezident. Tento pověřenec poskytuje informace a poradenství, kontroluje plnění povinností v oblasti ochrany osobních údajů, přijímá stížnosti a žádosti subjektů údajů a je kontaktním místem pro Úřad pro ochranu osobních údajů. Ochrana údajů tak není vnímána pouze jako technický problém informačních systémů, ale i jako součást vnitřního dohledu a odpovědnosti policejní organizace.

Neméně podstatná jsou práva subjektu údajů, i když v policejní oblasti podléhají určitým omezením. Zákon č. 110/2019 Sb. vychází z toho, že spravující orgán musí žádosti subjektu údajů vyřizovat bez zbytečného odkladu, nejdéle však do 60 dnů, současně však připouští omezení některých práv, pokud je to nezbytné ke splnění účelu zpracování. Zvláštní úprava se týká zejména přístupu, opravy, výmazu a omezení zpracování v případech, kdy by plné uplatnění těchto práv mohlo ohrozit nebo zmařit policejní účel zpracování. V policejním prostředí je proto nutné hledat rovnováhu mezi individuálními právy a veřejným zájmem.

Významnou součástí ochrany je rovněž kvalita a správnost údajů. Zákon o Policii ČR stanoví, že nepřesné osobní údaje nelze zpřístupňovat nebo předávat a že neověřené údaje musí být při zpřístupnění nebo předání označeny a doplněny o míru jejich spolehlivosti. V policejním prostředí je tento požadavek obzvlášť významný, protože práce s nepřesnými nebo neověřenými údaji může mít přímý dopad na práva konkrétní osoby.

Dalším důležitým prvkem je kontrola přístupů a logování operací. Zákon č. 110/2019 Sb. ukládá při automatizovaném zpracování pořizovat záznamy alespoň o operacích shromáždění, vložení, pozměnění, kombinování, nahlédnutí, předání, sdělení a výmazu osobních údajů. Tyto záznamy musí umožnit určit důvod a čas operace, totožnost osoby, která ji provedla, a v zásadě i příjemce údajů. Právě auditní stopa

umožňuje zpětně kontrolovat, zda byl přístup k údajům oprávněný a zda s nimi nebylo nakládáno v rozporu se zákonem.

Ochranu osobních údajů dále posiluje povinnost pravidelně prověřovat potřebnost dalšího zpracování. Zákon o Policii ČR výslovně stanoví, že policie nejméně jednou za tři roky prověří, zda jsou osobní údaje zpracovávané pro bezpečnostní a trestněprávní účely nadále potřebné. V policejním prostředí tak ochrana osobních údajů nespočívá jen v tom, že jsou údaje bezpečně uloženy, ale i v tom, že nejsou uchovávány déle, než je skutečně nezbytné.

Nezbytnou součástí ochrany je i zabezpečení systémů. Zákon č. 110/2019 Sb. ukládá spravujícímu orgánu přijmout taková technická a organizační opatření, aby zajistil a doložil splnění povinností při ochraně osobních údajů. Obecnou inspiraci poskytuje i článek 32 GDPR, který mezi vhodná opatření řadí například pseudonymizaci a šifrování, schopnost zajistit důvěrnost, integritu, dostupnost a odolnost systémů a proces pravidelného testování a hodnocení účinnosti zavedených opatření. Na úrovni doporučené praxe NÚKIB dlouhodobě zdůrazňuje význam řízení přístupu, auditů, bezpečnostních politik a pravidelného vyhodnocování bezpečnosti informačních systémů.

Zvláštní pozornost je nutné věnovat také porušení zabezpečení osobních údajů. Podle zákona č. 110/2019 Sb. spravující orgán ohlásí bez zbytečného odkladu porušení zabezpečení Úřadu pro ochranu osobních údajů, ledaže je riziko zásahu do práv a svobod subjektu údajů nízké. Pokud je toto riziko vysoké, má být incident oznámen i subjektu údajů, ledaže přijatá technická a organizační opatření zajišťují, že dotčené údaje nelze zneužít, nebo následná opatření významně snížila riziko. Tato úprava ukazuje, že bezpečnost databází není statický stav, ale proces, který musí počítat i s incidenty, jejich dokumentací a nápravou.

Ochrana osobních údajů v policejním prostředí je tedy vystavěna na několika navzájem propojených vrstvách: na zákonném vymezení účelu a rozsahu zpracování, na institucionálním dohledu, na omezeném, ale zachovaném systému práv subjektu údajů, na kvalitě a správnosti dat, na logování a kontrolní dohledatelnosti, na pravidelném přezkumu potřebnosti a na technickém i organizačním zabezpečení databází. Jde o komplexní právní a organizační režim, který má umožnit efektivní výkon policejních úkolů, aniž by se z databází stal nepřiměřený zásah do soukromí jednotlivce.

3.7 Nakládání s citlivými osobními údaji v policejních databázích

Na právní rámec vymezený v předchozí podkapitole bezprostředně navazuje otázka nakládání s citlivými osobními údaji v policejních databázích. Právě v této oblasti se nejvýrazněji projevuje zvláštní povaha policejního zpracování osobních údajů. Policie při plnění svých úkolů nepracuje pouze s běžnými identifikačními údaji, ale může se dostat i k údajům, které zasahují do velmi citlivé sféry soukromí fyzické osoby. Z tohoto důvodu je nakládání s těmito údaji podřízeno přísnějším pravidlům než zpracování běžných osobních údajů a musí být vždy vázáno na konkrétní zákonný účel, zásadu nezbytnosti a přiměřenosti.

V policejním prostředí je rozhodující především zvláštní zákonná úprava obsažená v § 79 zákona o Policii České republiky. Ta výslovně stanoví, že údaje o rasovém nebo etnickém původu, náboženském, filozofickém nebo politickém přesvědčení, členství v odborové organizaci, zdravotním stavu, sexuálním chování nebo sexuální orientaci lze shromažďovat pouze tehdy, je-li to nezbytné pro účely šetření konkrétního trestného činu nebo přestupku nebo při poskytování ochrany osob. Citlivé údaje tak v policejních databázích nemohou být vedeny plošně nebo preventivně bez konkrétního vztahu k zákonnému účelu policejní činnosti.

Z uvedeného vyplývá, že nakládání s citlivými osobními údaji v policejních databázích je založeno především na zásadě nezbytnosti. Policie nemůže tyto údaje shromažďovat jen proto, že by mohly být někdy užitečné, ale pouze tehdy, pokud jsou skutečně potřebné pro plnění konkrétního úkolu. Tato zásada je podstatná zejména proto, že citlivé údaje mají ve srovnání s běžnými osobními údaji vyšší vypovídací hodnotu a jejich zneužití může mít závažnější důsledky pro soukromí, důstojnost i právní postavení dotčené osoby.[14]

Vedle samotného shromažďování je důležitý i způsob dalšího nakládání s těmito údaji. Zákon o Policii České republiky současně požaduje, aby údaje zpracovávané pro trestněprávní a bezpečnostní účely byly vedeny odděleně od údajů zpracovávaných při plnění jiných úkolů policie. Tím se posiluje přehlednost právního režimu jednotlivých údajů a současně se omezuje riziko, že citlivé informace budou využity mimo účel, pro který byly získány.

[14] POLICIE ČESKÉ REPUBLIKY. Zpracování osobních údajů Policií České republiky [online]. Praha: Policie České republiky, [cit. 26. 3. 2026]. Dostupné z WWW: https://policie.gov.cz/clanek/zpracovani-osobnich-udaju-policii-ceske-republiky.aspx

Významné je také to, že zvláštní právní úprava dopadá nejen na samotné uchovávání údajů, ale i na výkon práv subjektu údajů a na kontrolu správnosti vedených informací. Zákon č. 110/2019 Sb. pro režim příslušných orgánů upravuje možnost opravy, omezení zpracování nebo výmazu osobních údajů a zároveň připouští omezení některých práv subjektu údajů tehdy, pokud by jejich plné uplatnění ohrozilo nebo zmařilo účel policejního zpracování.

Nakládání s citlivými údaji v policejních databázích je zároveň úzce spojeno s odpovědností za jejich přesnost, zabezpečení a kontrolovatelnost. Protože jde o údaje zvlášť citlivé, musí být zvýšená pozornost věnována tomu, kdo s nimi pracuje, v jakém rozsahu k nim přistupuje a jak je zaznamenána každá operace s nimi. Právě v tomto směru se nakládání s citlivými údaji propojuje s bezpečnostními opatřeními a kontrolními mechanismy, jimž je věnována následující podkapitola.

Lze tedy uzavřít, že nakládání s citlivými osobními údaji v policejních databázích představuje oblast, v níž se zvlášť výrazně střetává zájem na ochraně společnosti se zájmem na ochraně soukromí jednotlivce. Právní úprava proto připouští zpracování těchto údajů pouze v nezbytném rozsahu, za konkrétním zákonným účelem a v přísnějším režimu než u běžných osobních údajů.

3.8 Bezpečnostní opatření a kontrolní mechanismy

Bezpečnostní opatření a kontrolní mechanismy tvoří v policejních databázích jednu z nejdůležitějších podmínek zákonného a odpovědného nakládání s osobními údaji. V policejním prostředí se pracuje s informacemi, které mohou významně zasahovat do soukromí jednotlivce, a proto nestačí, aby byly databáze pouze technicky funkční. Musí být současně chráněny před neoprávněným přístupem, zneužitím, ztrátou, poškozením nebo neoprávněným předáváním údajů. Bezpečnost policejních databází proto nelze chápat jen jako technickou otázku, ale jako souhrn právních, organizačních, personálních i technických pravidel, která mají zajistit důvěrnost, správnost a dostupnost údajů.

Základním předpokladem ochrany údajů je omezení přístupu pouze na oprávněné osoby. S údaji vedenými v policejních databázích mohou pracovat jen ti pracovníci, kteří je skutečně potřebují k plnění konkrétních služebních úkolů. Rozsah přístupu by měl vždy odpovídat pracovnímu zařazení, druhu vykonávané činnosti a míře oprávnění konkrétní

osoby. Tím se snižuje riziko neoprávněného nahlížení do databáze nebo využití údajů mimo stanovený účel.

S přístupem k údajům úzce souvisí také spolehlivé ověřování totožnosti uživatelů. Nestačí pouze určit, kdo může do systému vstupovat, ale je nutné také bezpečně rozlišit, kdo konkrétní operaci provedl. Každý vstup do systému a každá práce s údaji by měla být spojena s konkrétní osobou, aby bylo možné zpětně ověřit, kdo do databáze nahlížel, jaké údaje zobrazil a jakým způsobem s nimi nakládal.

V souvislosti s automatizovaným zpracováním osobních údajů je třeba zdůraznit, že ochrana databází nespočívá pouze v samotném technickém nastavení systému, ale i v zajištění takových podmínek, které zabrání neoprávněnému nebo nahodilému přístupu k údajům, jejich změně, ztrátě či jinému zneužití. U elektronicky vedených evidencí je významné zejména to, že s údaji lze rychle nakládat, kopírovat je, přenášet je nebo je spojovat s dalšími soubory, a proto musí být ochrana spojena s přesným vymezením oprávněných osob, zabezpečením přístupů a kontrolou jednotlivých operací. Současně nelze opomenout ani personální stránku ochrany, protože osoby jednající za správce nebo zpracovatele smějí s údaji nakládat pouze v rozsahu odpovídajícím jejich oprávnění a jsou vázány povinností mlčenlivosti.[15]

Vedle technického zabezpečení je důležité i průběžné zaznamenávání práce s údaji. Každá významná operace provedená v policejní databázi by měla být evidována tak, aby bylo možné zpětně zjistit, kdo, kdy a jakým způsobem s údaji nakládal. Takové záznamy mají zásadní význam pro kontrolu zákonnosti zpracování osobních údajů i pro posouzení případného pochybení.

Na evidenci práce s údaji navazuje pravidelná kontrola a vnitřní dohled. Bezpečnost databází nemůže být zajištěna jednorázovým nastavením systému, ale musí být průběžně ověřována. Je proto nutné pravidelně kontrolovat, zda jsou přístupová oprávnění nastavena správně, zda se s údaji nakládá v souladu se zákonem a zda bezpečnostní opatření odpovídají charakteru chráněných údajů.

Nelze opomenout ani organizační a personální opatření. Bezpečnost policejních databází totiž nezávisí pouze na kvalitě technického řešení, ale také na tom, jak odpovědně se k údajům chovají osoby, které s nimi pracují. Součástí ochrany proto

[15] MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy.* Praha: Leges, 2018. s. 109. ISBN 978-80-7502-275-2.

musí být jasně stanovená pravidla, vnitřní předpisy, poučení uživatelů a jejich pravidelné proškolování. Lidský faktor je v této oblasti zásadní, protože i technicky kvalitně zabezpečený systém může selhat v důsledku nepozornosti, nedbalosti nebo vědomého zneužití přístupu.

Důležitou součástí bezpečnostních opatření je také připravenost na mimořádné situace a bezpečnostní incidenty. Žádný systém nelze považovat za zcela bezrizikový, a proto musí být součástí ochrany i postupy pro řešení případů, kdy dojde k neoprávněnému přístupu, úniku údajů, technickému výpadku nebo jinému narušení bezpečnosti. V takových situacích je nezbytné nejen incident zaznamenat, ale také rychle přijmout opatření ke zmírnění jeho následků a zabránit jeho opakování.

V širším pohledu je zřejmé, že bezpečnostní opatření a kontrolní mechanismy v policejních databázích musí tvořit vzájemně propojený celek. Samotné omezení přístupu bez následné kontroly nestačí, stejně jako technické zabezpečení nemůže nahradit odpovědné chování uživatelů. Účinná ochrana vzniká teprve tehdy, když jsou správně nastaveny přístupové režimy, technická ochrana, evidence operací, vnitřní kontrola, pravidelné prověřování a školení osob, které s databázemi pracují.

Bezpečnostní opatření a kontrolní mechanismy představují nezbytnou podmínku fungování policejních databází. Nejde o doplňkovou součást jejich provozu, ale o základní prvek, bez něhož by nebylo možné zajistit zákonné, odpovědné a důvěryhodné nakládání s údaji.

3.9 Rizika spojená se zpracováním osobních údajů

Zpracování osobních údajů v policejních databázích je spojeno s řadou rizik, která vyplývají jak z povahy samotných údajů, tak z účelu, pro který jsou shromažďovány a dále využívány. Policejní databáze obsahují informace, které mohou významně zasáhnout do soukromí jednotlivce, do jeho pověsti, osobní bezpečnosti i do jeho procesního postavení. Právě proto je nezbytné vnímat je nejen jako nástroj veřejné moci, ale také jako oblast se zvýšeným rizikem zásahu do základních práv.

Prvním významným rizikem je nadměrné nebo nepřiměřené shromažďování údajů. Policejní praxe je přirozeně založena na získávání informací potřebných pro odhalování a objasňování protiprávní činnosti, avšak právě zde vzniká napětí mezi potřebou efektivního výkonu policie a ochranou soukromí jednotlivce. Pokud by byly údaje shromažďovány ve větším rozsahu, než je skutečně nezbytné, nebo bez dostatečné

vazby na konkrétní zákonný účel, mohlo by dojít k nepřiměřenému zásahu do práva na ochranu osobních údajů.

Dalším podstatným rizikem je neoprávněný přístup k údajům a jejich vnitřní zneužití. Policejní databáze využívá větší počet oprávněných osob, a čím širší je okruh uživatelů a čím rozsáhlejší je obsah databáze, tím vyšší je i riziko, že dojde k nahlížení do údajů bez věcného důvodu nebo k jejich využití mimo služební účel. Právě z tohoto důvodu právní úprava počítá s vedením záznamů o operacích při automatizovaném zpracování a s možností zpětně ověřit, kdo, kdy a jak s osobními údaji nakládal.

Významné riziko představují také vnější bezpečnostní hrozby, zejména kybernetické útoky, úniky dat, poškození databází nebo ztráta jejich dostupnosti. V prostředí policejních databází může mít takový incident závažné následky nejen pro soukromí dotčených osob, ale i pro samotný výkon policejní činnosti. Pokud by došlo k úniku dat o probíhajících řízeních, o chráněných osobách nebo o jiných citlivých skutečnostech, mohl by být ohrožen veřejný zájem i konkrétní osoby.

Dalším problémem je nepřesnost, neúplnost nebo neaktuálnost evidovaných údajů. V policejních databázích může mít i zdánlivě drobná nepřesnost závažné důsledky, protože databáze slouží jako podklad pro další úkony, rozhodování a operativní činnost. Chybný údaj může vést k nesprávné identifikaci osoby, k nepřiměřenému zásahu nebo k dalšímu šíření informace, která neodpovídá skutečnosti. Riziko nesprávných údajů tak nespočívá jen v technické chybě evidence, ale i v možném zásahu do práv konkrétní osoby.

Zvláštní skupinu rizik tvoří nadměrná doba uchovávání údajů a nedostatečný přezkum jejich další potřebnosti. Policejní databáze mají přirozenou tendenci kumulovat údaje, a právě zde vzniká riziko, že budou vedeny i informace, které už nejsou potřebné, a přesto mohou nadále působit na právní postavení nebo soukromí dotčené osoby. Proto právní úprava ukládá pravidelně prověřovat, zda jsou osobní údaje zpracovávané pro bezpečnostní a trestněprávní účely nadále potřebné.

Ještě intenzivněji se tato rizika projevují u biometrických a genetických údajů, například u daktyloskopických údajů nebo profilů kyseliny deoxyribonukleové. Tyto údaje mají mimořádnou identifikační sílu a jejich zpracování proto představuje citelnější zásah do soukromí než vedení běžných evidenčních údajů. Riziko zde nespočívá

jen v samotném získání citlivého údaje, ale i v jeho dalším uchovávání, propojování a budoucím využívání.

Samostatným rizikem je také propojování údajů z více evidencí a vytváření širšího informačního obrazu o jednotlivci. Síla moderních policejních databází nespočívá jen v uchovávání samostatných údajů, ale i v možnosti jejich kombinace, sdružování a analytického využití. Z hlediska ochrany soukromí tak vzniká riziko, že propojením více údajů vznikne výrazně podrobnější profil osoby, než jaký by vyplýval z jednotlivých evidencí odděleně.

Nelze opomenout ani závislost policejní činnosti na funkčnosti databází a informačních systémů. Čím více jsou policejní procesy digitalizovány, tím větší dopad může mít technický výpadek, ztráta dat, porucha systému nebo jeho dočasná nedostupnost. Nejde jen o riziko pro ochranu osobních údajů, ale i o riziko pro schopnost policie vykonávat její zákonné úkoly.

Rizika spojená se zpracováním osobních údajů v policejních databázích jsou tedy mnohovrstevnatá. Zahrnují riziko nepřiměřeného rozsahu shromažďovaných údajů, neoprávněného přístupu, vnějších bezpečnostních incidentů, nepřesnosti údajů, nadměrné doby uchovávání, nepřiměřeného zpracování biometrických a genetických údajů, propojování různých evidencí i provozní závislosti na informačních systémech. Právě proto musí být policejní databáze podřízeny nejen požadavku efektivity, ale i důsledné kontrole zákonnosti, přiměřenosti a bezpečnosti. Jen za těchto podmínek mohou zůstat legitimním nástrojem ochrany veřejného pořádku a bezpečnosti, aniž by nepřiměřeně zasahovaly do práv jednotlivce.

3.10 Shrnutí poznatků

Policejní databáze představují v současném bezpečnostním prostředí významný a prakticky nepostradatelný nástroj Policie České republiky. Umožňují systematické shromažďování, evidenci, vyhledávání a vyhodnocování údajů potřebných pro plnění zákonných úkolů policie. Současně však nejde pouze o technické prostředky pro ukládání informací, ale o součást širšího informačního a právního prostředí, v němž se propojuje výkon veřejné moci, ochrana bezpečnosti a nakládání s osobními údaji.

Z provedeného rozboru vyplynulo, že tyto databáze jsou účelově zaměřené a slouží zejména k ochraně veřejného pořádku a bezpečnosti, pátrání po osobách a věcech, odhalování a objasňování trestné činnosti a plnění dalších úkolů stanovených

právními předpisy. Současně bylo zřejmé, že policejní databázové prostředí netvoří jeden jednotný systém, ale soustava různých evidencí a informačních nástrojů, které se liší svým účelem, rozsahem i charakterem zpracovávaných údajů.

Významná pozornost byla věnována také právnímu rámci a ochraně osobních údajů. Bylo potvrzeno, že fungování policejních databází je založeno především na zákoně o Policii České republiky a na právní úpravě ochrany osobních údajů, která zdůrazňuje zásady zákonnosti, účelovosti, nezbytnosti a přiměřenosti. Zvláštní význam má tato úprava zejména tam, kde policie nakládá s citlivými osobními údaji nebo s údaji biometrickými a genetickými.

Podstatnou součástí rozboru byla i bezpečnostní opatření a kontrolní mechanismy. Ukázalo se, že účinná ochrana policejních databází nespočívá pouze v technickém zabezpečení, ale v souhrnu opatření zahrnujících omezení přístupu, evidenci operací, vnitřní kontrolu, pravidelné přezkoumávání potřebnosti uchovávaných údajů a odpovědný přístup osob, které s údaji pracují. Současně byla zdůrazněna i rizika spojená se zpracováním osobních údajů, zejména riziko neoprávněného přístupu, nepřesnosti údajů, nadměrného shromažďování informací nebo jejich nepřiměřeného uchovávání.

Policejní databáze jsou pro fungování moderní policie nezastupitelné, avšak jejich využívání musí být vždy spojeno s důsledným respektem k zákonným pravidlům a k ochraně soukromí. Zjištěné poznatky současně vytvářejí vhodný základ pro následující část práce, která bude zaměřena na nemocniční databáze a umožní následné porovnání obou sledovaných oblastí.

4 Nemocniční databáze

Nemocniční databáze představují významnou součást současného zdravotnictví, protože slouží k evidenci, uchovávání a zpracování údajů nezbytných pro poskytování zdravotních služeb. Prostřednictvím těchto databází jsou vedeny informace o pacientech, průběhu jejich vyšetření a léčby, hospitalizacích, provedených zdravotních výkonech, laboratorních výsledcích, medikaci i dalších skutečnostech souvisejících se zdravotním stavem fyzických osob. V podmínkách moderního zdravotnictví již nelze efektivní poskytování zdravotní péče bez existence těchto databází prakticky zajistit.

Jejich význam nespočívá pouze v uchovávání údajů, ale především v možnosti jejich systematického uspořádání, vyhledávání, aktualizace a vzájemného propojení. Díky tomu lze zajistit návaznost zdravotní péče, přesnější diagnostiku, účelnější léčebný postup i efektivnější organizaci práce zdravotnického zařízení. Současně je však třeba zdůraznit, že nemocniční databáze obsahují značné množství osobních údajů, včetně údajů zvlášť citlivé povahy, a proto je nezbytné klást důraz na zákonnost jejich zpracování, omezení přístupu a jejich důslednou ochranu.

Tato kapitola se zaměřuje na vymezení nemocničních databází, jejich účel, typy zpracovávaných údajů, právní rámec jejich fungování, okruh oprávněných osob a ochranu údajů v nemocničním prostředí. Právě tyto otázky jsou podstatné pro následné porovnání nemocničních databází s databázemi policejními a pro posouzení rozdílů i podobností v přístupech k ochraně citlivých osobních údajů.

4.1 Vymezení nemocničních databází a jejich význam

Nemocniční databáze lze chápat jako organizované soubory údajů vedené v rámci zdravotnických zařízení, které slouží k evidenci, uchovávání, zpracování a zpřístupňování informací potřebných pro poskytování zdravotních služeb. Nejde pouze o technické úložiště dat, ale o praktický nástroj, který zdravotnickým pracovníkům umožňuje systematicky pracovat s informacemi o pacientech, průběhu jejich vyšetření a léčby, provedených zdravotních výkonech, hospitalizaci i dalších skutečnostech významných pro poskytování zdravotní péče.

Jejich postavení v rámci zdravotnického prostředí je mimořádně významné. Umožňují rychlou orientaci v údajích, jejich průběžnou aktualizaci a návazné využití při diagnostice, léčbě i organizaci péče. Zákon o zdravotních službách v této souvislosti vychází z toho, že zdravotnická dokumentace je souborem informací vedených,

zpracovávaných a uchovávaných poskytovatelem za účelem poskytování zdravotních služeb konkrétnímu pacientovi a že může být vedena i v elektronické podobě.[16]

Nemocniční databáze jsou úzce spojeny se zdravotnickou dokumentací, která tvoří jejich obsahové jádro. Právě jejím prostřednictvím jsou evidovány informace o zdravotním stavu pacienta a o skutečnostech souvisejících s poskytováním zdravotních služeb. Tyto databáze proto nelze chápat odděleně od zdravotnické dokumentace, ale spíše jako prostředí, v němž je tato dokumentace vedena, spravována a využívána.

Současně je třeba zdůraznit, že nemocniční databáze obsahují údaje mimořádně citlivého charakteru. GDPR výslovně řadí údaje o zdravotním stavu mezi zvláštní kategorie osobních údajů, a právě tato skutečnost odůvodňuje zvýšené požadavky na zákonnost zpracování, omezení okruhu oprávněných osob a technická a organizační opatření chránící tyto údaje před neoprávněným přístupem, ztrátou nebo zneužitím.

4.2 Účel nemocničních databází

Účel nemocničních databází je úzce spojen s poskytováním zdravotních služeb a s potřebou systematicky zaznamenávat, uchovávat a využívat údaje vztahující se ke konkrétnímu pacientovi. Základní smysl těchto databází spočívá v tom, že umožňují soustředit na jednom místě informace nezbytné pro diagnostiku, léčbu, sledování zdravotního stavu pacienta i pro návaznost další zdravotní péče.

Jedním z hlavních účelů nemocničních databází je zajištění kontinuity a návaznosti zdravotní péče. V nemocničním prostředí se na poskytování zdravotních služeb zpravidla podílí více zdravotnických pracovníků, často i více oddělení nebo odborností současně. Aby mohla být péče poskytována řádně a bezpečně, je nezbytné, aby byly důležité informace o pacientovi dostupné včas, v odpovídajícím rozsahu a v přehledné podobě.

Dalším významným účelem je podpora diagnostiky a rozhodování zdravotnických pracovníků. Přehledně vedené a průběžně doplňované údaje umožňují lékařům i dalším oprávněným osobám získat ucelený obraz o zdravotním stavu pacienta,

[16] ČESKO. Zákon č. 372 ze dne 6. listopadu 2011 o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách). In: Sbírka zákonů, Česká republika. 2011, částka 131, s. 4729–4904. Dostupné z WWW: <https://www.psp.cz/sqw/sbirka.sqw?cz=372&r=2011>. ISSN 1211-1244.

jeho předchozí léčbě, výsledcích vyšetření i o případných rizicích spojených s dalším léčebným postupem.

Databáze však neslouží pouze k samotnému poskytování zdravotní péče. Jejich účel je také evidenční, organizační a administrativní. Umožňují vést přehled o přijetí a propuštění pacientů, hospitalizacích, ambulantních návštěvách, vykázaných výkonech, objednávání pacientů a předávání informací mezi jednotlivými pracovišti. Současně plní významnou funkci při plnění zákonných povinností poskytovatele zdravotních služeb.

4.3 Typy údajů zpracovávaných v nemocničních databázích.

Nemocniční databáze zpracovávají široké spektrum údajů, které souvisejí s poskytováním zdravotních služeb pacientovi a s organizací zdravotní péče v rámci zdravotnického zařízení. Jejich obsah nelze zúžit pouze na informace o diagnóze či léčbě, protože zahrnují také údaje identifikační, kontaktní, administrativní a provozní.

První významnou skupinu tvoří identifikační a kontaktní údaje pacienta, zejména jméno a příjmení, datum narození, rodné číslo, číslo pojištěnce, kód zdravotní pojišťovny, adresa pobytu, telefonní číslo a adresa elektronické pošty. Vedle údajů vztahujících se přímo k pacientovi se v databázích objevují také údaje o poskytovateli zdravotních služeb, oddělení zdravotnického zařízení a zdravotnickém pracovníkovi, který provedl zápis.

Další, a z hlediska ochrany soukromí nejvýznamnější, skupinu tvoří údaje o zdravotním stavu pacienta. Sem patří zejména anamnestické údaje, informace o průběhu a výsledku poskytovaných zdravotních služeb, pracovní závěry a konečná diagnóza, výsledky laboratorních, zobrazovacích a dalších vyšetření, operační protokoly, anesteziologické záznamy, údaje o dosavadní léčbě a reakci pacienta na ni i návrhy dalšího léčebného postupu.[17]

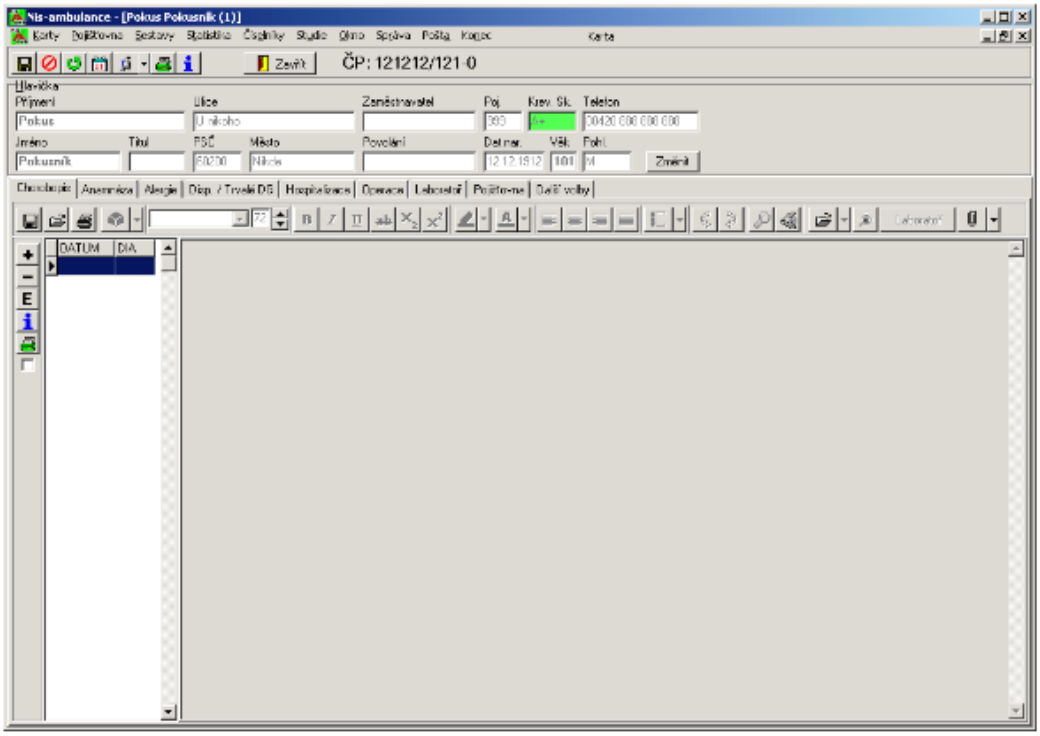
Nemocniční databáze zároveň zahrnují i údaje související s organizací a právním průběhem zdravotní péče. Evidují se například datum a čas přijetí pacienta do péče, datum a čas ukončení péče, údaje o přeložení na jiné oddělení nebo k jinému poskytovateli,

[17] ČESKO. MINISTERSTVO ZDRAVOTNICTVÍ. Vyhláška č. 444 ze dne 19. prosince 2024 o zdravotnické dokumentaci. In: Sbírka zákonů a mezinárodních smluv, Česká republika. 2024, akt č. 444/2024 Sb. Dostupné z WWW: <https://www.e-sbirka.cz/sb/2024/444>. ISSN 3029-5092.

záznamy o informovaném souhlasu, o odmítnutí zdravotních služeb nebo o použití omezovacích prostředků.

Z hlediska ochrany osobních údajů je podstatné, že značná část údajů vedených v nemocničních databázích spadá do zvláštní kategorie osobních údajů. Vedle údajů o zdravotním stavu se v nemocničním prostředí mohou vyskytovat také genetické údaje a v některých případech i biometrické údaje. Typologie těchto údajů tak ukazuje, že nejde pouze o běžnou evidenci pacientů, ale o komplexní soubor informací, jehož ochrana má zásadní význam z právního i etického hlediska.

Obrázek 3: Nemocniční databáze



Zdroj: Karlovarská Krajská nemocnice

4.4 Právní rámec nemocničních databází

Právní rámec nemocničních databází je vícevrstevný a tvoří jej jak obecná právní úprava ochrany osobních údajů, tak zvláštní předpisy upravující poskytování zdravotních služeb, vedení zdravotnické dokumentace, elektronizaci zdravotnictví a v určitých případech také kybernetickou bezpečnost. Nemocniční databáze proto nelze posuzovat pouze z hlediska technického fungování, ale především jako prostředí, ve kterém dochází ke zpracování osobních údajů o vysoké citlivosti a v němž se současně uplatňují požadavky na zákonnost, důvěrnost, bezpečnost a dostupnost údajů. Základ tohoto rámce tvoří na evropské úrovni GDPR, v českém právním řádu zejména zákon č. 110/2019 Sb.,

o zpracování osobních údajů, zákon č. 372/2011 Sb., o zdravotních službách, vyhláška č. 444/2024 Sb., o zdravotnické dokumentaci, a dále také zákon č. 325/2021 Sb., o elektronizaci zdravotnictví. U některých poskytovatelů mohou být významné rovněž povinnosti vyplývající z nové právní úpravy kybernetické bezpečnosti. [18]

Z obecného hlediska je rozhodující nařízení Evropského parlamentu a Rady (EU) 2016/679, tedy GDPR, které stanoví základní zásady zpracování osobních údajů, zejména zákonnost, korektnost, transparentnost, účelové omezení, minimalizaci údajů, omezení uložení a integritu a důvěrnost. GDPR zároveň výslovně řadí údaje o zdravotním stavu mezi zvláštní kategorie osobních údajů a jejich zpracování v zásadě zakazuje, ledaže je splněna některá z výjimek stanovených v čl. 9 odst. 2. Pro oblast zdravotnictví je klíčová zejména výjimka pro lékařskou diagnostiku, poskytování zdravotní péče, léčbu a řízení systémů a služeb zdravotní péče, a dále výjimka pro veřejný zájem v oblasti veřejného zdraví. Současně GDPR předpokládá, že takové údaje jsou zpracovávány osobami vázanými povinností mlčenlivosti nebo na jejich odpovědnost. V nemocničním prostředí proto zpravidla nejde o zpracování založené jen na souhlasu pacienta, ale především o zpracování opřené o právní povinnost a zvláštní zákonné důvody pro nakládání s údaji o zdravotním stavu.

Na úrovni českého právního řádu na GDPR navazuje zákon č. 110/2019 Sb., o zpracování osobních údajů. Tento zákon představuje adaptační předpis, který doplňuje unijní rámec a upravuje některé otázky ochrany osobních údajů v podmínkách České republiky. Pro nemocniční databáze má význam zejména tím, že potvrzuje použitelnost obecného režimu ochrany osobních údajů i v oblasti zdravotnictví a spolu s GDPR vytváří základní právní rámec, v němž se musí pohybovat každý poskytovatel zdravotních služeb jako správce osobních údajů.

Zvláštní a pro nemocniční databáze stěžejní právní úpravu obsahuje zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování. Tento zákon upravuje samotné poskytování zdravotních služeb, práva a povinnosti pacientů i poskytovatelů a současně stanoví pravidla pro vedení, zpracování a uchovávání zdravotnické dokumentace. Právě zdravotnická dokumentace tvoří obsahové jádro nemocničních databází, protože jde o soubor informací vedených a uchovávaných

[18] NÁRODNÍ CENTRUM ELEKTRONICKÉHO ZDRAVOTNICTVÍ. Národní strategie elektronického zdravotnictví [online]. Praha: Ministerstvo zdravotnictví České republiky, bez data [cit. 26. 3. 2026]. Dostupné z WWW: https://ncez.mzcr.cz/cs/narodni-strategie-elektronickeho-zdravotnictvi/narodni-strategie-elektronickeho-zdravotnictvi

poskytovatelem za účelem poskytování zdravotních služeb konkrétnímu pacientovi. Zákon zároveň upravuje povinnost mlčenlivosti zdravotnických pracovníků a dalších osob, pravidla nahlížení do zdravotnické dokumentace i možnost vedení dokumentace v elektronické podobě. Aktuální právní úprava navíc výslovně počítá s tím, že informační systém, ve kterém je zdravotnická dokumentace vedena elektronicky, musí umožnit její převod do výstupního datového formátu stanoveného standardem elektronického zdravotnictví.

Na zákon o zdravotních službách navazuje prováděcí předpis, kterým je nově vyhláška č. 444/2024 Sb., o zdravotnické dokumentaci. Ta nahradila dřívější vyhlášku č. 98/2012 Sb., která byla zrušena k 1. lednu 2025. Nová vyhláška podrobně upravuje obsah zdravotnické dokumentace, její členění, způsob vedení, zapisování údajů, opravy záznamů, dobu uchování i postup při vyřazování zdravotnické dokumentace. Pro nemocniční databáze je tato vyhláška zásadní proto, že konkretizuje, jaké údaje mají být v dokumentaci vedeny a jak má být dokumentace formálně i obsahově vedena, a tím nepřímo vymezuje i požadavky kladené na nemocniční databáze jako prostředí, v němž jsou tyto údaje evidovány a spravovány.

Významnou součástí právního rámce je rovněž zákon č. 325/2021 Sb., o elektronizaci zdravotnictví. Tento zákon upravuje elektronické zdravotnictví a stanoví podmínky pro bezpečné sdílení dat v jeho rámci. Současně vychází z toho, že elektronické zdravotnictví zahrnuje nejen služby a informační systémy Integrovaného datového rozhraní zdravotnictví, ale také informační systémy poskytovatelů zdravotních služeb sloužící k vedení nebo předávání zdravotnické dokumentace v elektronické podobě. Ve vazbě na zákon o zdravotních službách má význam zejména pro pacientský souhrn, standardizaci elektronických výstupů a bezpečné předávání zdravotních údajů mezi oprávněnými subjekty. Tato právní úprava tak reaguje na rostoucí digitalizaci zdravotnictví a posiluje právní rámec pro elektronické vedení a sdílení údajů obsažených v nemocničních databázích.

Vedle ochrany osobních údajů a zdravotnické dokumentace je dnes nutné zohlednit i požadavky kybernetické bezpečnosti. Od 1. listopadu 2025 je účinný nový zákon č. 264/2025 Sb., o kybernetické bezpečnosti. Tato úprava nedopadá automaticky na každého poskytovatele zdravotních služeb, ale může se vztahovat na ty subjekty, které naplní kritéria regulované služby. Pro tyto organizace pak znamená další povinnosti v oblasti řízení bezpečnostních opatření, hlášení incidentů a komunikace s Národním

úřadem pro kybernetickou a informační bezpečnost. V prostředí nemocničních databází má tato právní úprava význam zejména proto, že vedle ochrany soukromí zdůrazňuje i odolnost informačních systémů vůči kybernetickým hrozbám a požadavek zachování dostupnosti a integrity zdravotních údajů.

Právní rámec nemocničních databází je tvořen souborem navzájem propojených předpisů, které sledují několik souběžných cílů. Na jedné straně chrání soukromí pacienta a zákonnost zpracování jeho osobních údajů, na straně druhé upravují vedení zdravotnické dokumentace, bezpečné sdílení údajů v elektronickém zdravotnictví a u části poskytovatelů i kybernetickou bezpečnost informačních systémů. Právě tato kombinace obecných i zvláštních právních pravidel činí z nemocničních databází oblast, v níž se zvlášť výrazně prolíná ochrana osobních údajů, zdravotnické právo a bezpečnost informačních technologií.

4.5 Přístup k údajům vedeným v nemocničních databázích

Přístup k údajům vedeným v nemocničních databázích představuje jednu z nejvýznamnějších otázek ochrany osobních údajů ve zdravotnictví. Nemocniční databáze obsahují nejen běžné identifikační údaje pacienta, ale především údaje o jeho zdravotním stavu, průběhu léčby, výsledcích vyšetření a dalších skutečnostech, které patří mezi zvláštní kategorie osobních údajů. Z tohoto důvodu nemůže být přístup k těmto údajům neomezený, ale musí být vázán na zákonem stanovený důvod, postavení konkrétní osoby a účel, pro který je do údajů nahlíženo.

Základní oprávněnou osobou je sám pacient. Ten má právo do své zdravotnické dokumentace nahlížet, pořizovat si z ní výpisy nebo kopie a rozhodovat také o tom, komu dalšímu bude přístup umožněn. U nezletilých pacientů a u osob omezených ve svéprávnosti vykonává tato oprávnění zpravidla zákonný zástupce nebo opatrovník.

Vedle pacienta a jím určených osob mají k údajům vedeným v nemocničních databázích přístup také zdravotničtí pracovníci, kteří se podílejí na poskytování zdravotních služeb. Tento přístup je odůvodněn samotným účelem zdravotnické dokumentace, současně však nejde o oprávnění neomezené. Přístup má být vázán na pracovní zařazení, konkrétní úkol a nezbytný rozsah údajů potřebných pro poskytování péče.

Další skupinu tvoří subjekty, které mohou do zdravotnické dokumentace nahlížet i bez souhlasu pacienta, pokud je k tomu výslovně zmocňuje zákon. Nejde však

o prolomení ochrany údajů v obecné rovině, ale o zákonem vymezené výjimky, které musí být vykládány restriktivně.

S přístupem k údajům úzce souvisí povinnost mlčenlivosti. Samotné oprávnění nahlížet do dokumentace neznamená právo s údaji dále volně nakládat nebo je sdělovat jiným osobám. Přístup k údajům je vždy třeba spojovat s odpovědností za jejich ochranu a s povinností využívat je výlučně k účelu, pro který byly zpřístupněny.

V prostředí elektronizovaného zdravotnictví navíc nabývá na významu i technické řízení přístupových oprávnění. Elektronické zdravotnictví tak posiluje nejen dostupnost údajů pro oprávněné osoby, ale i kontrolu pacienta nad tím, kdo k jeho údajům přistupuje, a umožňuje auditování a monitoring přístupů. Právě tato kombinace právních a technických pravidel je podstatná pro ochranu citlivých osobních údajů pacienta v nemocničním prostředí.

4.6 Ochrana údajů v nemocničních databázích a související rizika

Ochrana údajů v nemocničních databázích představuje jednu z nejdůležitějších podmínek jejich zákonného a bezpečného fungování. Důvodem je zejména skutečnost, že v tomto prostředí dochází ve velkém rozsahu ke zpracování údajů o zdravotním stavu, které GDPR řadí mezi zvláštní kategorie osobních údajů a kterým proto přiznává zvýšenou míru ochrany. Správce je povinen přijímat taková opatření, aby zpracování probíhalo zákonně, bezpečně a pouze v rozsahu odpovídajícím účelu, pro který jsou údaje vedeny. Ochrana údajů v nemocničních databázích tak není pouze technickou otázkou, ale představuje soubor právních, organizačních a bezpečnostních pravidel, jejichž cílem je chránit soukromí pacienta i důvěryhodnost zdravotnického zařízení.

Základní požadavky na zabezpečení vyplývají především z čl. 25 a čl. 32 GDPR. Ty ukládají správci a zpracovateli přijmout vhodná technická a organizační opatření s ohledem na stav techniky, náklady na provedení, povahu, rozsah, kontext a účel zpracování i na rizika pro práva a svobody fyzických osob. V nemocničním prostředí se tato povinnost promítá zejména do zabezpečení informačních systémů, řízení přístupových oprávnění, ochrany před neoprávněným nahlížením do zdravotnické dokumentace, zálohování dat a do nastavení vnitřních kontrolních mechanismů.

Vedle neoprávněného přístupu k údajům a rizika jejich úniku se jako významné problematické okruhy ukazují také kybernetické hrozby, nedostatečné nastavení přístupových oprávnění a lidský faktor. Právě zdravotnická zařízení patří mezi subjekty,

u nichž může mít bezpečnostní incident zvlášť závažné dopady, neboť může ohrozit nejen důvěrnost citlivých údajů, ale i samotnou dostupnost zdravotních služeb. Ochrana údajů v nemocničních databázích proto musí být založena na souběžném působení právních, technických i organizačních opatření, která zajistí důvěrnost, integritu, dostupnost a bezpečnost zpracovávaných údajů.

Na význam kybernetické bezpečnosti v širším systémovém kontextu upozorňuje také Národní strategie kybernetické bezpečnosti 2026–2030. Ta vymezuje kybernetickou bezpečnost jako oblast, v níž je třeba posilovat bezpečnost a odolnost informačních a komunikačních systémů a současně zvyšovat odolnost vůči hrozbám v kyberprostoru.[19] Strategie zároveň vytváří jednotný a koordinovaný rámec, který zdůrazňuje, že ochranu citlivých informací nelze oddělit od celkového zabezpečení systémů, nastavení odpovědností a připravenosti institucí na bezpečnostní incidenty. Tyto závěry jsou významné i pro nemocniční databáze, neboť potvrzují, že ochrana osobních údajů ve zdravotnictví nemůže být chápána izolovaně, ale jako součást širšího systému informační a kybernetické bezpečnosti.

Význam uvedeného přístupu je v nemocničním prostředí o to větší, že zde dochází ke střetu dvou legitimních požadavků. Na jedné straně stojí potřeba rychlé dostupnosti údajů pro poskytování zdravotní péče, na straně druhé nutnost zamezit neoprávněnému přístupu, zneužití či úniku těchto informací. Čím více jsou zdravotnické služby závislé na elektronických databázích a propojených informačních systémech, tím větší význam má důsledné řízení přístupových oprávnění, průběžná kontrola přístupů, ochrana proti kybernetickým útokům a pravidelné vyhodnocování bezpečnostních rizik.

Vedle technických opatření je nezbytné zdůraznit také význam organizační stránky ochrany údajů. Nedostatečně nastavená interní pravidla, nejednotný postup zaměstnanců nebo selhání lidského faktoru mohou oslabit i jinak kvalitně zabezpečený systém. Ochrana údajů v nemocničních databázích proto předpokládá nejen odpovídající technické zabezpečení, ale i pravidelné školení zaměstnanců, jasné vymezení odpovědnosti a důslednou kontrolu dodržování vnitřních pravidel při práci s citlivými údaji.

[19] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Národní strategie kybernetické bezpečnosti 2026–2030* [online]. Brno: NÚKIB, 2025 [cit. 25. 3. 2026]. Dostupné z WWW: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2026-2030.pdf

Lze tedy uzavřít, že ochrana údajů v nemocničních databázích musí být chápána komplexně. Nestačí pouze formální existence právních pravidel nebo technické zabezpečení systému, ale je nezbytné, aby byla tato pravidla důsledně uplatňována v každodenní praxi zdravotnických zařízení. Právě propojení právního rámce, technických opatření, organizačních pravidel a odpovědného přístupu zaměstnanců představuje základní předpoklad bezpečného vedení nemocničních databází. Nemocniční databáze tak představují specifickou oblast zpracování citlivých osobních údajů, v níž se mimořádně výrazně prolínají požadavky na efektivní poskytování zdravotní péče a požadavek důsledné ochrany soukromí pacienta. Tato skutečnost je činí vhodným předmětem následné komparace s databázemi policejními, neboť ačkoli oba typy databází pracují s citlivými údaji, činí tak v odlišném účelovém, institucionálním i právním rámci.

4.7 Shrnutí poznatků

Nemocniční databáze představují v současném zdravotnictví nezastupitelný nástroj pro evidenci, uchovávání a zpracování údajů nezbytných pro poskytování zdravotních služeb. Jejich význam nespočívá pouze v technickém ukládání informací, ale především v tom, že umožňují systematickou práci s údaji o pacientech, průběhu diagnostiky, léčby, hospitalizace i dalších skutečnostech souvisejících se zdravotním stavem fyzických osob.

Z provedeného rozboru vyplynulo, že nemocniční databáze jsou úzce spojeny se zdravotnickou dokumentací, obsahují široké spektrum citlivých údajů a jsou podřízeny vícevrstevnému právnímu rámci tvořenému předpisy o ochraně osobních údajů, zdravotních službách, zdravotnické dokumentaci i elektronizaci zdravotnictví. Přístup k těmto údajům proto nemůže být neomezený, ale musí být vázán na zákonem stanovený důvod, účel a okruh oprávněných osob.

Současně bylo zdůrazněno, že ochrana údajů v nemocničních databázích nespočívá pouze v technickém zabezpečení, ale v souhrnu právních, technických a organizačních opatření. Právě tato skutečnost činí nemocniční databáze vhodným předmětem následné komparace s databázemi policejními, neboť ačkoli oba typy databází pracují s citlivými údaji, činí tak v odlišném účelovém, institucionálním i právním rámci.

5 Ochrana citlivých údajů a bezpečnostní postupy v databázích

Problematika ochrany citlivých údajů představuje jednu z nejvýznamnějších otázek současné informační společnosti. Databáze, v nichž jsou shromažďovány a dále zpracovávány údaje o fyzických osobách, mohou obsahovat informace mimořádně citlivého charakteru, jejichž neoprávněné zpřístupnění, zneužití nebo ztráta mohou závažně zasáhnout do soukromí, důstojnosti i dalších práv dotčených osob. V odborné literatuře jsou za základní cíle informační bezpečnosti považovány důvěrnost, integrita a dostupnost informací.[20] Zvýšenou pozornost je proto třeba věnovat nejen samotnému právnímu režimu těchto údajů, ale také bezpečnostním postupům a opatřením, jejichž cílem je právě ochrana důvěrnosti, integrity a dostupnosti informací vedených v databázích. GDPR výslovně vymezuje zvláštní kategorie osobních údajů a spojuje s nimi zvýšenou ochranu právě proto, že jejich zpracování může vytvářet významná rizika pro práva a svobody fyzických osob.

Význam této problematiky je zvlášť patrný v prostředí policejních a nemocničních databází. V obou případech totiž dochází ke zpracování údajů, které mohou vypovídat o zdravotním stavu, biometrických znacích, identitě nebo jiných skutečnostech citlivě zasahujících do soukromé sféry člověka. Současně však platí, že ochrana těchto údajů nemůže být chápána pouze jako překážka jejich využívání, neboť v řadě případů je jejich zpracování nezbytné pro plnění zákonných úkolů, poskytování zdravotních služeb nebo zajištění veřejné bezpečnosti. Právní úprava proto hledá rovnováhu mezi požadavkem na ochranu soukromí a potřebou zákonného a účelného nakládání s údaji.

5.1 Vymezení citlivých údajů a právní rámec jejich ochrany

Při vymezení citlivých údajů je nejprve nutné vycházet z obecnějšího pojmu osobní údaj. Osobním údajem je každá informace, která se vztahuje ke konkrétní fyzické osobě a umožňuje její přímou nebo nepřímou identifikaci. Rozhodující tedy není jen samotný obsah informace, ale také možnost spojit ji s určitým člověkem. Ochrana osobních údajů je přitom v právním smyslu spojena se žijící fyzickou osobou, k níž se zpracovávané údaje vztahují.[21]

[20] PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence a MARGULIES, Jonathan. *Security in Computing*. 5th ed. Boston: Pearson, 2015, s. 40–41. ISBN 978-0-13-408504-3.
[21] MELOTÍKOVÁ, Petra. *Osobní údaje v kontextu GDPR.* Praha: Leges, 2020. s. 64. ISBN 978-80-7502-507-4.

Na tento obecný pojem navazuje užší skupina údajů, které právní úprava považuje za zvlášť citlivé. V současné právní terminologii je označení citlivé údaje nahrazováno pojmem zvláštní kategorie osobních údajů. Obecné nařízení o ochraně osobních údajů mezi ně řadí zejména údaje vypovídající o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém přesvědčení, členství v odborech, genetické údaje, biometrické údaje zpracovávané za účelem jedinečné identifikace fyzické osoby, údaje o zdravotním stavu a údaje týkající se sexuálního života nebo sexuální orientace fyzické osoby. U těchto údajů je požadována zvýšená ochrana, protože jejich zneužití může mít závažné důsledky pro soukromí, důstojnost, společenské postavení i bezpečnost dotčené osoby.

Právní rámec ochrany zvláštních kategorií osobních údajů vychází především z obecného nařízení o ochraně osobních údajů. To stanoví základní zásady zpracování osobních údajů, zejména zákonnost, korektnost a transparentnost, účelové omezení, minimalizaci údajů, přesnost, omezení uložení a zásadu integrity a důvěrnosti. U zvláštních kategorií osobních údajů současně vychází z obecného zákazu jejich zpracování, od něhož připouští pouze zákonem stanovené výjimky. Zpracování těchto údajů je proto možné jen tehdy, existuje-li k němu odpovídající právní důvod, například v oblasti zdravotní péče, ochrany veřejného zdraví nebo na základě jiného zvláštního zákonného titulu. Na evropskou úpravu v českém právním řádu navazuje zákon č. 110/2019 Sb., o zpracování osobních údajů, který obecný rámec ochrany osobních údajů dále rozvíjí v podmínkách České republiky.

Ve zdravotnictví je ochrana citlivých údajů dále konkretizována zvláštními právními předpisy. Zásadní význam má zejména zákon č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, který upravuje vedení zdravotnické dokumentace, práva a povinnosti poskytovatelů zdravotních služeb i pacientů a vytváří základní rámec pro nakládání s údaji o zdravotním stavu. Na něj navazuje vyhláška č. 444/2024 Sb., o zdravotnické dokumentaci, která podrobněji upravuje obsah a způsob vedení zdravotnické dokumentace. Významnou roli má rovněž zákon č. 325/2021 Sb., o elektronizaci zdravotnictví, jenž stanoví podmínky pro bezpečné fungování elektronického zdravotnictví a pro sdílení údajů v jeho rámci. V nemocničním prostředí tedy ochrana citlivých údajů nespočívá pouze v obecném režimu ochrany osobních údajů, ale je úzce spojena i se zvláštní právní úpravou zdravotních služeb a zdravotnické dokumentace.

Odlišná situace nastává v policejním prostředí. U zpracování osobních údajů pro účely předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů nebo zajišťování veřejného pořádku se neuplatní obecný režim ochrany osobních údajů ve stejné podobě jako v běžné správní či soukromé sféře. Tato oblast je v českém právu upravena zejména v hlavě třetí zákona č. 110/2019 Sb., která dopadá na zpracování osobních údajů příslušnými orgány pro takzvané policejní účely. Současně je třeba zohlednit i zákon č. 273/2008 Sb., o Policii České republiky, který policii opravňuje zpracovávat osobní údaje v nezbytném rozsahu pro plnění jejích zákonných úkolů. Ochrana citlivých údajů se tak v policejních databázích odvíjí od odlišného účelového a institucionálního rámce než ve zdravotnictví, přesto však i zde platí požadavek zákonnosti, nezbytnosti a přiměřenosti zpracování.

Z uvedeného vyplývá, že ochrana citlivých údajů v databázích stojí na dvou vzájemně propojených rovinách. První z nich představuje obecná právní úprava ochrany osobních údajů, která stanoví základní principy a limity jejich zpracování. Druhou rovinu tvoří zvláštní právní úprava jednotlivých oblastí, v nichž se s citlivými údaji pracuje, zejména zdravotnictví a policejní činnosti. Právě propojení těchto dvou rovin je rozhodující pro posouzení, za jakých podmínek mohou být citlivé údaje v databázích shromažďovány, uchovávány, zpřístupňovány a chráněny.

5.2 Bezpečnostní postupy a opatření k ochraně údajů

Ochrana citlivých údajů v databázích nemůže být založena pouze na existenci právní úpravy, ale musí být zajištěna také konkrétními bezpečnostními postupy a opatřeními. GDPR v této souvislosti ukládá správcům a zpracovatelům povinnost zavádět vhodná technická a organizační opatření, a to jak při navrhování zpracování, tak i v jeho průběhu. Současně požaduje, aby úroveň zabezpečení odpovídala rizikům, která mohou pro práva a svobody fyzických osob vzniknout.

Mezi výslovně uváděná opatření patří například pseudonymizace a šifrování osobních údajů, schopnost zajistit důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování, schopnost obnovit dostupnost údajů po incidentu a pravidelné testování a hodnocení přijatých opatření.

5.2.1 Technická opatření

Mezi technická opatření k ochraně osobních údajů patří nejen zabezpečení databázových systémů proti neoprávněnému přístupu, ale také takové postupy,

které snižují možnost identifikace konkrétní fyzické osoby. Významnou roli v této souvislosti hraje anonymizace údajů. Jejím smyslem je upravit data tak, aby již nebylo možné určit, ke komu se vztahují, a to ani prostřednictvím dalších dostupných informací. Pokud je anonymizace provedena skutečně účinně, přestávají být takto upravené údaje osobními údaji v právním smyslu.

Současně je však třeba zdůraznit, že za anonymizované nelze považovat každé údaje, u nichž byly odstraněny pouze některé přímé identifikátory. Při posuzování anonymizace je důležité zohlednit i možnost nepřímé nebo zpětné identifikace osoby, například propojením s dalšími údaji. Právě proto musí být anonymizace chápána jako odborný technický postup, jehož účinnost je třeba posuzovat s ohledem na konkrétní okolnosti a na reálnou možnost znovu určit totožnost dotčené osoby.

V prostředí databází má anonymizace význam zejména tam, kde je potřebné pracovat s daty pro analytické, statistické nebo jiné účely, aniž by bylo nutné zachovat vazbu na konkrétní fyzickou osobu. Takové opatření přispívá ke zvýšení ochrany soukromí a současně naplňuje požadavek, aby byly zpracovávány jen údaje v rozsahu skutečně nezbytném pro daný účel. Technická opatření tedy nespočívají pouze v ochraně systému jako takového, ale i v úpravě dat tak, aby bylo co nejvíce omezeno riziko zásahu do práv dotčených osob.[22]

5.2.2 Organizační opatření

Vedle technických opatření je při ochraně osobních údajů nezbytné věnovat pozornost také opatřením organizačním. Ta zahrnují zejména nastavení vnitřních pravidel, rozdělení odpovědnosti, způsob přístupu k údajům, kontrolu pohybu dokumentů a celkové uspořádání činností v rámci organizace. Ochrana osobních údajů totiž nespočívá pouze v zabezpečení informačních systémů, ale také v tom, jak je v praxi organizována práce s údaji, kdo k nim má přístup a za jakých podmínek jsou uchovávány nebo předávány.

V této souvislosti je důležité, aby ochrana údajů byla součástí širšího bezpečnostního režimu organizace. Ten může zahrnovat nejen elektronické zabezpečení, ale i fyzickou ochranu prostor, v nichž jsou údaje zpracovávány nebo ukládány. Význam

[22] NULÍČEK, Michal; DONÁT, Josef; NONNEMANN, František; LICHNOVSKÝ, Bohuslav; TOMÍŠEK, Jan**.** *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. s. 117. ISBN 978-80-7552-765-3.

má zejména kontrola vstupu do chráněných prostor, oddělení jednotlivých úrovní ochrany a nastavení takových pravidel, která snižují riziko neoprávněného přístupu k osobním údajům. Taková opatření mají význam zejména tam, kde se s citlivými údaji pracuje jak v elektronické, tak i v listinné podobě.

Součástí organizačních opatření je také správné nastavení práce s dokumenty. V praxi totiž stále nelze vycházet pouze z předpokladu, že všechny údaje budou vedeny výhradně elektronicky. Mnohé instituce i nadále pracují s listinnými dokumenty, které obsahují osobní údaje a které je třeba chránit obdobně jako databázové záznamy. Ochrana údajů proto zahrnuje také pravidla pro vytváření, evidenci, ukládání, vyhledávání, předávání a případnou archivaci dokumentů. Důležité je, aby byl celý tento proces přehledně nastaven a aby bylo zřejmé, kdo za jednotlivé fáze nakládání s dokumenty odpovídá.[23]

Organizační opatření tak představují důležitý doplněk opatření technických. Jejich smyslem je vytvořit takové provozní a vnitřní podmínky, které omezí riziko ztráty, zneužití nebo neoprávněného zpřístupnění osobních údajů. V prostředí policejních i nemocničních databází to znamená zejména potřebu jasně vymezených pravidel, odpovědného zacházení s dokumentací a návaznosti mezi fyzickou, elektronickou a personální ochranou údajů.

5.2.3 Řízení přístupových oprávnění a řešení incidentů

Jedním z nejdůležitějších praktických bezpečnostních postupů je řízení přístupových oprávnění. Citlivé údaje nesmějí být zpřístupněny každé osobě, která má technickou možnost vstoupit do systému, ale pouze těm, které je nezbytně potřebují pro plnění svých úkolů. S tím souvisí i požadavek evidence přístupů a auditovatelnosti činností prováděných v databázi. V oblasti elektronického zdravotnictví je tento princip výslovně posílen i systémovými nástroji. Národní centrum elektronického zdravotnictví uvádí, že Registr oprávnění umožňuje občanovi nastavit práva k nahlížení do dokumentace a k zastupování, zatímco Žurnál činností slouží k centralizovanému zaznamenávání a uchovávání informací o provedených činnostech oprávněných osob a funguje jako auditní a logovací subsystém. Tyto nástroje ukazují, že moderní ochrana citlivých údajů se neobejde bez přesné evidence toho, kdo k údajům přistupoval a jak s nimi nakládal.

[23] NAVRÁTIL, Jiří a kol. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018. s. 231. ISBN 978-80-7380-689-7.

Řešení incidentů představuje další nezbytnou součást bezpečnostních postupů. V případě databází obsahujících citlivé údaje může mít bezpečnostní incident podobu neoprávněného přístupu, úniku dat, ztráty dostupnosti systému nebo kybernetického útoku. NÚKIB dlouhodobě upozorňuje, že zdravotnická zařízení patří mezi cíle kybernetických útoků a že obdobné hrozby mohou vážně ohrozit fungování nemocnic a dalších významných subjektů. Reakce na incident proto musí zahrnovat nejen technické zvládnutí situace, ale i právní a organizační kroky, tedy vyhodnocení dopadů, případné ohlášení porušení zabezpečení a přijetí opatření, která sníží pravděpodobnost opakování. Bezpečnostní postupy v databázích tak musí být nastaveny jako průběžný proces, nikoli jako jednorázové opatření.

Bezpečnostní postupy a opatření k ochraně citlivých údajů v databázích musí spojovat technickou ochranu systému, organizační pravidla práce s údaji, přesné řízení přístupových oprávnění i připravenost na incidenty. Teprve souběh těchto prvků může zajistit, že databáze budou nejen funkční a využitelné, ale současně i bezpečné a v souladu s požadavky právní úpravy ochrany osobních údajů.

5.3 Rizika spojená se zpracováním citlivých údajů

Se zpracováním citlivých údajů v databázích jsou neoddělitelně spojena rizika, která mohou zasáhnout jak do soukromí dotčených osob, tak do řádného fungování samotné instituce. U zvláštních kategorií osobních údajů je třeba vycházet z toho, že případné porušení zabezpečení může mít zpravidla závažnější následky než u běžných osobních údajů. Obecné nařízení o ochraně osobních údajů proto při zabezpečení zpracování výslovně vyžaduje zohlednit rizika náhodného nebo protiprávního zničení, ztráty, pozměnění, neoprávněného zpřístupnění nebo neoprávněného přístupu k osobním údajům. Do popředí se tak dostává zejména ochrana důvěrnosti, integrity a dostupnosti údajů.

Jedním z nejzávažnějších rizik je neoprávněný přístup k údajům. K tomu může dojít jak zvenčí, tedy působením osob bez oprávnění, tak i uvnitř organizace, pokud jsou přístupová oprávnění nastavena příliš široce nebo nejsou dostatečně kontrolována. U databází obsahujících údaje o zdravotním stavu, biometrické údaje nebo jiné citlivé informace může neoprávněné seznámení se s jejich obsahem představovat vážný zásah do soukromí člověka a vyvolat i další negativní následky.

Další významnou skupinu rizik představují únik dat, jejich ztráta nebo poškození. Porušení zabezpečení osobních údajů se nemusí projevit pouze kybernetickým útokem na databázi, ale také ztrátou listinných dokumentů, chybným zasláním údajů neoprávněnému adresátovi nebo poškozením datového nosiče. Riziko tedy nespočívá pouze v samotném informačním systému, ale i v praktickém nakládání s údaji při jejich přenosu, tisku, archivaci nebo běžné administrativní práci.

V současném digitálním prostředí nelze opomenout ani kybernetické hrozby. Národní úřad pro kybernetickou a informační bezpečnost dlouhodobě upozorňuje zejména na phishing, spear phishing a ransomware, přičemž zdravotnictví je z povahy své činnosti a hodnoty zpracovávaných dat zvlášť citlivým sektorem. Kybernetický útok může vést nejen k úniku osobních údajů, ale také k jejich dočasné nebo trvalé nedostupnosti a k narušení provozu organizace. V nemocničním prostředí to může mít dopad i na poskytování zdravotních služeb, v policejním prostředí pak na výkon bezpečnostních úkolů a práci s evidencemi.

Významným zdrojem rizik je také lidský faktor. Ani technicky dobře zabezpečený systém totiž nezaručí dostatečnou ochranu údajů, pokud osoby, které s nimi pracují, nedodržují stanovené postupy, chybně nakládají s přístupovými údaji nebo podcení význam ochrany citlivých informací. Z tohoto důvodu mají zásadní význam organizační pravidla, pravidelná školení, kontrola přístupů, evidence operací a průběžné vyhodnocování bezpečnostních incidentů.

U zpracování citlivých údajů je proto nezbytné vycházet z preventivního přístupu, zejména tehdy, jsou-li údaje zpracovávány ve velkém rozsahu, systematicky, při využití nových technologií nebo při propojování více datových souborů. V takových případech může vznikat vysoké riziko pro práva a svobody fyzických osob. Právě z tohoto důvodu obecné nařízení o ochraně osobních údajů ukládá v určitých případech provést předem posouzení vlivu na ochranu osobních údajů, jehož účelem je popsat zamýšlené zpracování, posoudit jeho nezbytnost a přiměřenost, identifikovat možná rizika a navrhnout opatření, která povedou k jejich omezení na přijatelnou úroveň.[24]

Za hlavní rizika spojená se zpracováním citlivých údajů v databázích lze považovat neoprávněný přístup, únik nebo ztrátu údajů, kybernetické útoky

[24] STAŇKOVÁ, Lucie. *GDPR snadno a přehledně.* Praha: Mladá fronta, 2018. s. 129. ISBN 978-80-204-5108-8.

a pochybení lidského faktoru. U databází obsahujících citlivé údaje je proto nezbytné průběžně vyhodnocovat možná rizika a přijímat taková technická a organizační opatření, která jejich vznik omezí a minimalizují jejich dopady.

6 Porovnání přístupů policejních a nemocničních databází k ochraně citlivých údajů a možnosti vzájemné inspirace v bezpečnostních strategiích

Policejní a nemocniční databáze představují dva odlišné typy informačních systémů, které však spojuje skutečnost, že v jejich rámci dochází ke zpracování osobních údajů vysoké citlivosti. V obou případech jde o údaje, jejichž neoprávněné zpřístupnění, zneužití nebo ztráta mohou mít závažné důsledky pro dotčené osoby i pro fungování příslušných institucí. Přestože policejní a nemocniční databáze vznikají v rozdílném institucionálním a právním prostředí a sledují odlišné účely, lze mezi nimi nalézt jak významné společné znaky, tak i podstatné rozdíly.

Cílem této kapitoly je porovnat přístupy policejních a nemocničních databází k ochraně citlivých údajů, zejména z hlediska účelu zpracování údajů, právního rámce, okruhu oprávněných osob a používaných bezpečnostních opatření. Současně bude pozornost věnována i tomu, zda a v jakém směru mohou být bezpečnostní strategie obou prostředí vzájemně inspirativní. Komparace těchto dvou oblastí je významná zejména proto, že umožňuje lépe vystihnout specifika ochrany citlivých údajů v jednotlivých typech databází a současně poukázat na možné přínosy sdílení osvědčených postupů.

6.1 Společné znaky policejních a nemocničních databází

Policejní a nemocniční databáze představují na první pohled odlišné informační celky, neboť vznikají v rozdílném institucionálním prostředí a slouží odlišným účelům. Přesto mezi nimi existuje řada společných znaků, které odůvodňují jejich vzájemné porovnání z hlediska ochrany citlivých údajů. V obou případech jde o databáze, jejichž prostřednictvím jsou systematicky evidovány, uchovávány, tříděny a dále využívány údaje vztahující se ke konkrétním fyzickým osobám. Tyto údaje přitom mohou mít mimořádně citlivý charakter, neboť vypovídají například o zdravotním stavu, identitě, biometrických znacích, protiprávním jednání, bezpečnostních rizicích nebo jiných skutečnostech významně zasahujících do soukromé sféry jednotlivce.

Dalším společným znakem obou typů databází je jejich zásadní význam pro fungování příslušné instituce. Policejní databáze tvoří důležitou informační základnu pro plnění úkolů Policie České republiky, zejména v oblasti prevence, odhalování a objasňování protiprávního jednání, pátrání po osobách a věcech nebo zajišťování veřejného pořádku. Nemocniční databáze obdobně představují nezbytný nástroj pro poskytování zdravotních služeb, vedení zdravotnické dokumentace, návaznost péče a organizaci činnosti zdravotnického zařízení. V obou případech tedy nejde pouze o technické úložiště dat, ale o funkční nástroj, bez něhož by bylo řádné plnění úkolů dané instituce podstatně obtížnější, nebo dokonce nemožné.

Společným rysem policejních i nemocničních databází je rovněž to, že přístup k vedeným údajům nemůže být neomezený. Naopak je nutné, aby byl vázán na zákonný důvod, pracovní zařazení konkrétní osoby a účel, pro který jsou údaje využívány. V obou prostředích proto vystupuje do popředí požadavek omezeného a kontrolovaného přístupu, řízení přístupových oprávnění a odpovědnosti těch osob, které s údaji pracují. S tím úzce souvisí také nutnost evidence přístupů a kontrolních mechanismů, které umožňují zpětně ověřit, kdo s údaji nakládal a zda tak činil v souladu se zákonem a vnitřními pravidly.

Významným společným znakem je i zvýšený požadavek na zabezpečení těchto databází. V obou případech musí být chráněna důvěrnost, integrita a dostupnost údajů, neboť neoprávněný přístup, ztráta, poškození nebo únik dat mohou mít závažné důsledky nejen pro dotčenou osobu, ale i pro fungování celé instituce. Policejní databáze i nemocniční databáze jsou proto spojeny s potřebou zavádění technických a organizačních opatření, jako je řízení přístupových oprávnění, autentizace uživatelů, zálohování dat, kontrola činnosti oprávněných osob nebo postupy pro řešení bezpečnostních incidentů.

Společné je také to, že v obou prostředích hraje významnou roli lidský faktor. Ani kvalitní technické zabezpečení samo o sobě nezaručuje ochranu údajů, pokud osoby, které s nimi pracují, nedodržují stanovené postupy, překračují rozsah svého oprávnění nebo podceňují význam ochrany citlivých informací. Právě proto je v policejním i nemocničním prostředí nezbytné spojovat technické zabezpečení databází

s organizačními pravidly, školením zaměstnanců a důslednou kontrolou dodržování stanovených povinností.[25]

Policejní a nemocniční databáze spojuje zejména práce s citlivými údaji o fyzických osobách, jejich zásadní význam pro činnost příslušné instituce, požadavek zákonného a omezeného přístupu k údajům a potřeba vysoké úrovně jejich zabezpečení. Právě tyto společné znaky vytvářejí základ pro další komparaci, která se zaměří na rozdíly v účelu, právním rámci, rozsahu zpracovávaných údajů i v konkrétních bezpečnostních postupech obou typů databází.

6.2 Rozdíly v účelu a právním rámci obou typů databází

Zásadní rozdíl mezi policejními a nemocničními databázemi spočívá v účelu jejich existence. Nemocniční databáze slouží především k poskytování zdravotních služeb, vedení zdravotnické dokumentace, zajištění návaznosti péče a organizaci činnosti zdravotnického zařízení. Jejich hlavním smyslem je ochrana zdraví a života pacienta a podpora diagnostiky a léčby. Naproti tomu policejní databáze slouží k plnění úkolů Policie České republiky, zejména v oblasti předcházení, vyhledávání a odhalování trestné činnosti, pátrání po osobách a věcech a zajišťování veřejného pořádku. Zatímco nemocniční databáze tedy sledují léčebný a evidenční účel, policejní databáze jsou spojeny s výkonem veřejné moci v oblasti bezpečnosti.

Odlišný účel se promítá i do právního rámce. V nemocničním prostředí se uplatní zejména obecný režim ochrany osobních údajů podle GDPR a zákona č. 110/2019 Sb., doplněný zvláštní právní úpravou zdravotnictví, především zákonem č. 372/2011 Sb., o zdravotních službách, a navazující vyhláškou o zdravotnické dokumentaci. V policejním prostředí je zpracování osobních údajů upraveno zvláštním režimem podle hlavy III zákona č. 110/2019 Sb. a současně zákonem č. 273/2008 Sb., o Policii České republiky, který policii opravňuje zpracovávat osobní údaje pro plnění jejích zákonných úkolů.

Rozdíl je patrný také v povaze zpracovávaných údajů. V nemocničních databázích převažují údaje o zdravotním stavu, diagnózách, výsledcích vyšetření, léčbě a hospitalizaci. V policejních databázích jsou naopak vedeny údaje potřebné pro bezpečnostní a pořádkové účely, tedy zejména údaje identifikační, popisné,

[25] ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ. Zdravotnictví [online]. Praha: ÚOOÚ, [cit. 26. 3. 2026]. Dostupné z WWW: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2026-2030.pdf.

kontaktní, případně biometrické nebo jiné údaje významné pro policejní činnost. Odlišný je rovněž okruh oprávněných osob. V nemocničním prostředí je přístup k údajům vázán především na zdravotnické pracovníky a na pacienta, zatímco v policejním prostředí je spojen zejména s policií a dalšími oprávněnými orgány veřejné moci.

Hlavní rozdíly mezi oběma typy databází spočívají v účelu zpracování, právním režimu, povaze vedených údajů a okruhu oprávněných osob. Nemocniční databáze jsou zaměřeny na poskytování zdravotní péče, zatímco policejní databáze na ochranu bezpečnosti a veřejného pořádku. Tyto odlišnosti se následně promítají i do konkrétních bezpečnostních postupů a ochranných opatření.

6.3 Porovnání bezpečnostních postupů a ochranných opatření

Policejní i nemocniční databáze spojuje požadavek vysoké úrovně zabezpečení, protože v obou případech jde o systémy obsahující citlivé údaje o fyzických osobách. V obou prostředích je proto nezbytné zajistit omezený přístup k údajům, kontrolu oprávnění, evidenci práce s daty a ochranu před neoprávněným zpřístupněním, ztrátou nebo zneužitím. Obecný rámec těchto opatření vyplývá z právní úpravy ochrany osobních údajů, která klade důraz na bezpečnost zpracování, přiměřenost opatření a odpovědnost správce.

V nemocničním prostředí je ochrana údajů úzce spojena se zdravotnickou dokumentací a s právem pacienta na kontrolu přístupu k údajům o jeho zdravotním stavu. Zákon o zdravotních službách vychází z toho, že zdravotnická dokumentace je vedena za účelem poskytování zdravotních služeb konkrétnímu pacientovi, a současně stanoví povinnost zaznamenat každé nahlédnutí do dokumentace nebo poskytnutí údajů oprávněnému subjektu. V rámci elektronického zdravotnictví je tento princip dále posílen například Registrem oprávnění, který umožňuje spravovat souhlasy a přístupová práva k nahlížení do zdravotnické dokumentace.

V policejním prostředí je naopak ochrana údajů více spojena s plněním bezpečnostních úkolů státu a s kontrolovatelností jednotlivých úkonů při zpracování údajů. Zákon o zpracování osobních údajů výslovně dopadá i na zpracování prováděné příslušnými orgány pro policejní účely a zákon o Policii České republiky váže zpracování osobních údajů na plnění konkrétních úkolů policie. Současně ukládá uchovávat informace o čase, příjemci a důvodech zpřístupnění nebo předání osobních údajů a pravidelně prověřovat, zda jsou zpracovávané údaje nadále potřebné. Ve srovnání

s nemocničním prostředím je tedy v policejní praxi výraznější důraz na účelové omezení, auditovatelnost a průběžné přezkoumávání potřebnosti dalšího zpracování.

V obou typech databází se uplatňují obdobné bezpečnostní principy, zejména omezení přístupu, evidence práce s údaji a požadavek odpovídajícího technického i organizačního zabezpečení. Rozdíl spočívá především v jejich těžišti. V nemocničním prostředí vystupuje více do popředí ochrana soukromí pacienta a možnost řídit přístup k údajům o jeho zdravotním stavu, zatímco v policejním prostředí je silnější akcent kladen na zákonný účel zpracování, kontrolu jednotlivých úkonů a průběžné ověřování potřebnosti uchovávaných údajů.

6.4 Možnosti vzájemné inspirace v bezpečnostních strategiích

Přestože policejní a nemocniční databáze fungují v odlišném účelovém i právním rámci, lze mezi nimi nalézt několik oblastí, v nichž mohou být jejich bezpečnostní strategie vzájemně inspirativní. Společným východiskem je zejména požadavek omezeného přístupu k údajům, evidence práce s daty a důsledné kontroly toho, kdo, kdy a z jakého důvodu s údaji nakládal. V obou prostředích je zároveň zřejmé, že ochrana citlivých údajů nemůže být založena pouze na obecném zákonném rámci, ale musí být podpořena konkrétními technickými a organizačními postupy.

Z nemocničního prostředí může být pro policejní praxi inspirativní zejména důraz na detailní správu oprávnění a na větší transparentnost přístupů k údajům. V elektronickém zdravotnictví je tento princip posílen například Registrem oprávnění, který umožňuje nastavovat práva k nahlížení do dokumentace a k zastupování, a Žurnálem činností, který funguje jako auditní a logovací subsystém zaznamenávající provedené činnosti oprávněných osob. Tyto nástroje ukazují, jak významná je přesná evidence přístupů a možnost jejich následné kontroly.

Naopak z policejního prostředí může být pro zdravotnictví inspirativní důslednější akcent na průběžné přezkoumávání potřebnosti dalšího uchovávání a zpracování údajů. Pro policejní účely právní úprava zdůrazňuje účelové omezení, oddělení určitých režimů zpracování a také pravidelné prověřování potřebnosti dalšího zpracování osobních údajů. Tento přístup může být přínosný i pro nemocniční prostředí, zejména při posuzování rozsahu uchovávaných údajů, nastavení retenčních pravidel a pravidelném vyhodnocování, zda konkrétní přístupová oprávnění nebo rozsah zpracování stále odpovídají skutečné potřebě.

Pro obě oblasti je společně inspirativní také důraz na prevenci bezpečnostních incidentů, vzdělávání zaměstnanců a posilování bezpečnostní kultury. Samotné technické zabezpečení totiž nezaručí dostatečnou ochranu údajů, pokud nejsou správně nastavena organizační pravidla a pokud osoby pracující s daty nechápou význam svých povinností. Právě propojení technických opatření, jasně vymezených oprávnění, logování přístupů, pravidelné kontroly a průběžného školení zaměstnanců může představovat nejvýznamnější prostor pro vzájemnou inspiraci mezi policejním a nemocničním prostředím.

Možnosti vzájemné inspirace nespočívají v přebírání totožných pravidel, ale spíše v přenosu osvědčených principů. Nemocniční prostředí může být inspirativní v oblasti transparentnější správy oprávnění a evidence přístupů, zatímco policejní prostředí v důslednějším přezkoumávání potřebnosti zpracování a silnějším důrazu na účelové omezení údajů. V obou případech však platí, že účinná ochrana citlivých údajů je založena na propojení právních pravidel, technických opatření a odpovědného přístupu osob, které s údaji pracují.

7 Výzkumná sonda

Tato kapitola představuje praktickou část bakalářské práce a navazuje na poznatky uvedené v teoretické části. Jejím smyslem je doplnit právní a odborná východiska o praktický pohled na problematiku ochrany citlivých osobních údajů v databázích používaných v policejním a nemocničním prostředí. Praktická část je zaměřena na zkušenosti, názory a vnímání rizik u osob, které se s těmito databázemi ve své profesní činnosti setkávají.

Praktická část práce má průzkumný charakter a jejím cílem je přispět k lepšímu pochopení toho, jak je ochrana citlivých osobních údajů vnímána v praxi, jaká rizika jsou považována za nejzávažnější a ve kterých oblastech je spatřován prostor pro zlepšení současného stavu.

7.1 Cíl výzkumné sondy

Hlavním cílem výzkumné sondy je zjistit, jak pracovníci Policie České republiky a pracovníci nemocničních zařízení vnímají ochranu citlivých osobních údajů v databázích, se kterými při své profesní činnosti pracují, a identifikovat silné a slabé stránky současné praxe.

Dílčími cíli výzkumné sondy je:

- zjistit, jak respondenti hodnotí úroveň ochrany citlivých osobních údajů v databázích používaných v policejním a nemocničním prostředí,
- zmapovat, jaká rizika jsou při práci s těmito databázemi vnímána jako nejzávažnější,
- ověřit, zda respondenti považují technická a organizační opatření k ochraně údajů za dostatečná,
- identifikovat oblasti, ve kterých by bylo možné zvýšit bezpečnost a efektivitu databází obsahujících citlivé osobní údaje,
- zjistit, zda respondenti spatřují možnost vzájemné inspirace mezi policejním a nemocničním prostředím v oblasti ochrany údajů a bezpečnostních postupů.

7.2 Metoda výzkumné sondy

Pro účely výzkumné sondy byla zvolena metoda dotazníkového šetření. Tato metoda byla vybrána zejména proto, že umožňuje získat odpovědi od většího počtu respondentů v relativně krátkém čase a současně zajistit jednotnou strukturu zjišťovaných informací. Dotazník byl zaměřen na praktické zkušenosti respondentů s databázemi obsahujícími citlivé osobní údaje, na jejich hodnocení úrovně ochrany těchto údajů, na vnímaná rizika a na posouzení dostatečnosti technických a organizačních opatření využívaných v praxi.

Dotazníkové šetření bylo určeno výhradně pracovníkům Policie České republiky a pracovníkům nemocničních zařízení. Důvodem tohoto zaměření byla skutečnost, že právě tyto dvě profesní skupiny přicházejí ve své pracovní činnosti do kontaktu s databázemi obsahujícími citlivé osobní údaje, a mohou proto poskytnout relevantní praktické poznatky k ochraně těchto údajů a k fungování bezpečnostních opatření.

Dotazník byl tvořen výhradně uzavřenými otázkami, aby bylo možné odpovědi přehledně a jednoznačně vyhodnotit. Respondenti měli u každé otázky možnost vybrat vždy pouze jednu odpověď. Otázky se zaměřovaly zejména na četnost práce s databázemi, hodnocení úrovně ochrany citlivých údajů, přístupová oprávnění, školení zaměstnanců, nejvýznamnější rizika a možné směry zlepšení. Vzhledem k povaze bakalářské práce má výzkumná sonda průzkumný charakter. Jejím cílem není vytvořit obecně platné závěry pro všechny pracovníky policie a nemocnic, ale získat orientační přehled o tom, jak osoby z těchto dvou profesních prostředí vnímají ochranu citlivých údajů a bezpečnostní postupy v databázích, se kterými pracují.

7.3 Charakteristika respondentů

Respondenty výzkumné sondy tvoří pouze pracovníci Policie České republiky a pracovníci nemocničních zařízení. Do výzkumu byli zařazeni záměrně, neboť se jedná o osoby, které se ve své profesní činnosti setkávají s databázemi obsahujícími citlivé osobní údaje nebo s problematikou jejich ochrany.

U pracovníků policie lze předpokládat zkušenost s evidencemi a databázemi používanými při plnění úkolů v oblasti bezpečnosti, veřejného pořádku a odhalování protiprávního jednání. U pracovníků nemocničních zařízení lze naopak předpokládat zkušenost s databázemi a dokumentací využívanou při poskytování zdravotních služeb, vedení zdravotnické dokumentace a ochraně údajů o zdravotním stavu pacientů.

Vzhledem k rozsahu a charakteru bakalářské práce nelze výsledky výzkumné sondy považovat za statisticky reprezentativní pro všechny pracovníky Policie České republiky a všechny pracovníky nemocničních zařízení. Získané odpovědi však mohou poskytnout užitečný orientační přehled o tom, jak jsou ochrana citlivých osobních údajů, bezpečnostní opatření a související rizika vnímány v praxi právě v těchto dvou profesních prostředích.

7.4 Zpracování a vyhodnocení dat

Získaná data byla zpracována především deskriptivním způsobem. Odpovědi respondentů byly tříděny, porovnávány a následně vyhodnocovány s ohledem na stanovený cíl výzkumné sondy. U uzavřených otázek byly sledovány četnosti jednotlivých odpovědí, případně jejich procentuální vyjádření. U otevřených odpovědí byl kladen důraz na obsahové zachycení opakujících se názorů, zkušeností a problémových okruhů.

Při interpretaci výsledků bylo přihlíženo k tomu, že jde o průzkumnou sondu, jejímž smyslem je především identifikace tendencí a praktických poznatků, nikoli formulace zobecnitelných závěrů pro celou populaci.

7.5 Přínos výzkumné sondy pro bakalářskou práci

Výzkumná sonda představuje důležitou součást bakalářské práce, protože umožňuje propojit teoretické poznatky s praktickou zkušeností. Jejím přínosem je zejména to, že pomáhá odhalit, jak jsou ochrana citlivých údajů, bezpečnost databází a související rizika vnímány v reálné praxi. Získané poznatky mohou následně sloužit jako podklad pro formulaci závěrů práce a pro návrhy opatření, která by mohla přispět ke zvýšení bezpečnosti a efektivity databázových systémů.

7.6 Vytvoření hypotéz

Byly vytvořeny výzkumné předpoklady, jejichž potvrzení či vyvrácení bylo cílem výzkumné sondy.

Hypotéza 1: Ve většině případů se respondenti domnívají, že přístup k citlivým údajům mají pouze osoby, které je skutečně potřebují k výkonu své činnosti.

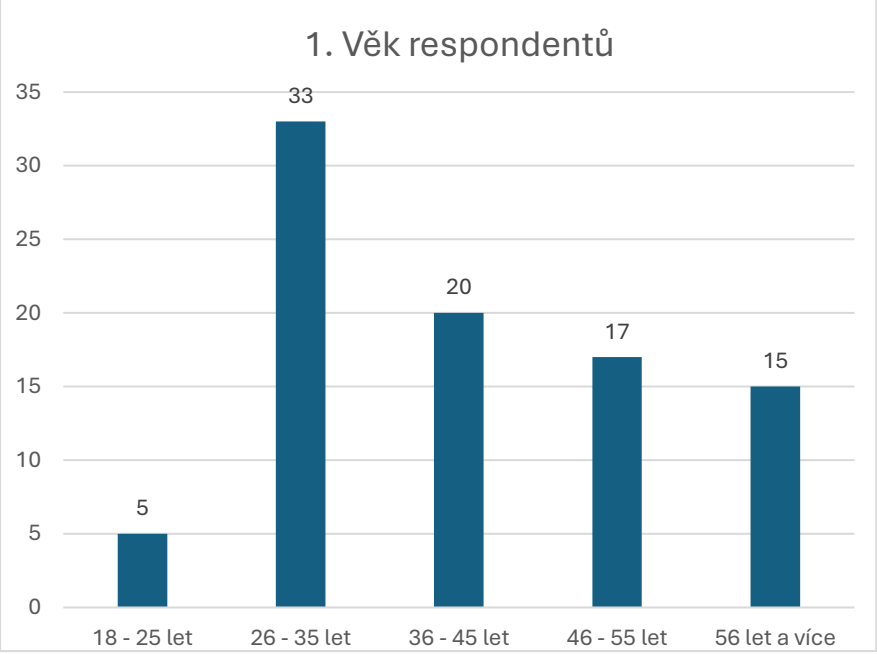
Hypotéza 2: Většina respondentů se domnívá, že ke zvýšení bezpečnosti citlivých údajů by nejvíce přispěla přísnější kontrola přístupových oprávnění a jasnější interní pravidla.

Hypotéza 3: Za nejzávažnější riziko při zpracování citlivých údajů v databázích považují respondenti nejčastěji neoprávněný přístup k údajům.

7.7 Identifikační údaje respondentů

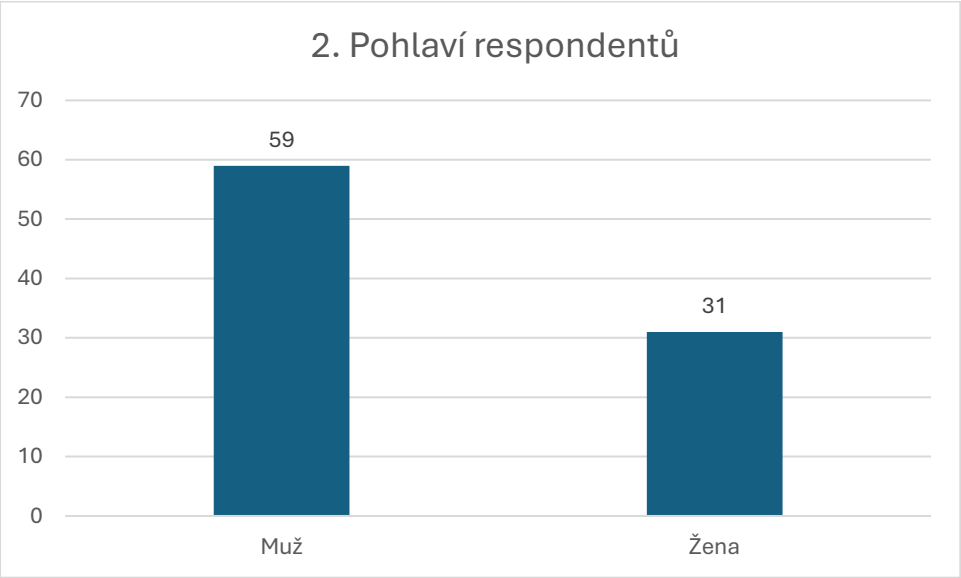
Dotazníkové šetření celkem vyplnilo 90 respondentů. První otázka se týkala věku respondentů. Ten byl rozdělen do pěti intervalů – od 18 do 25 let, od 26 do 35 let, od 36 do 45 let, od 46 do 55 let a od 56 let výše. Nejvíce respondentů bylo ve věkové skupině od 26 do 35 let a to celkem 33 respondentů (36,7 %). Nejméně lidí naopak označilo věk od 18 do 25 let, a to 5 respondentů (5,6 %). Druhou nejpočetnější skupinou byla kategorie od 36 do 45 let a to celkem 20 respondentů (22,2 %). V kategorii 46 – 55 let bylo cekem 17 respondentů (18,9 %) a kategorii od 56 let výše tvořilo 15 respondentů (16,7 %).

Obrázek 4: Věk respondentů



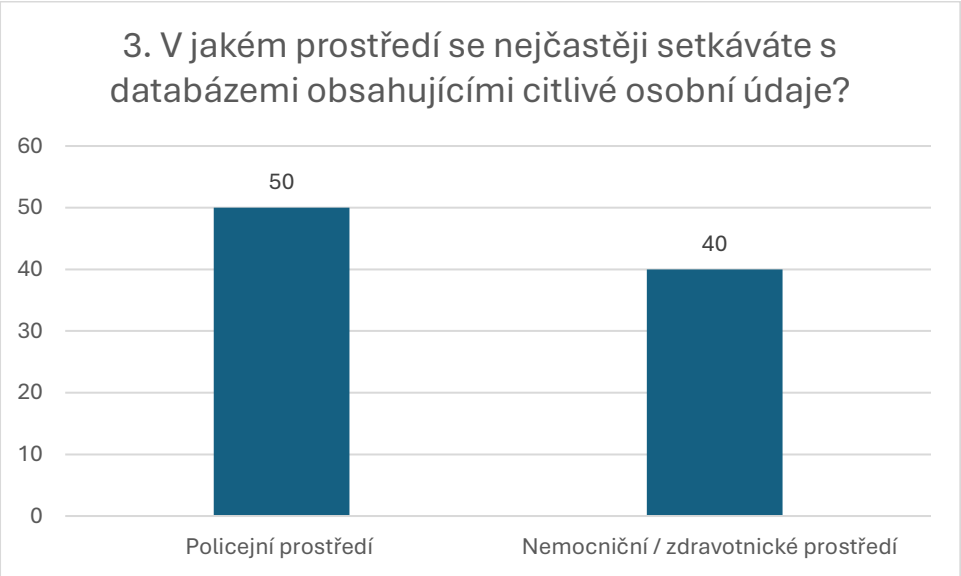
Co se týče pohlaví, převažovali muži. Těch vyplnilo dotazník 59, což představuje 65,6 % všech dotazovaných. Žen bylo pouze 31, tedy 34,4 %.

Obrázek 5: Pohlaví respondentů



Vzhledem k tématu bakalářské práce byli osloveni zaměstnanci policie a nemocničních zařízení. Policistů bylo 50, tedy 55,6 %. z řad nemocničního personálu se podařilo oslovit 40 pracovníků, což tvoří 44,4 %.

Obrázek 6: V jakém prostředí se nejčastěji setkáváte s databázeni obsahujícími citlivé osobní údaje?

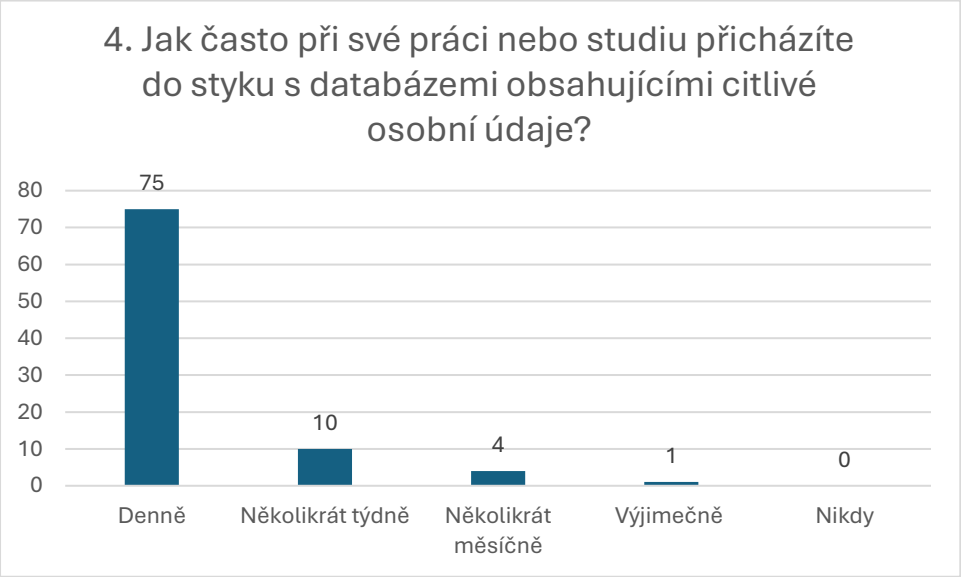


7.8 Vyhodnocení otázek k databázím s citlivými osobními údaji

Ve čtvrté otázce byli respondenti dotazováni jak často při své práci nebo studiu přichází do styku s databázemi obsahujícími citlivé osobní údaje.

75 respondentů (83,3 %) přichází do styku s databázemi obsahující citlivé osobní údaje denně, 10 respondentů (11,1 %) s nimi pracuje několikrát týdně, 4 respondenti (4,4 %) několikrát měsíčně a jediný respondent (1,1 %) výjimečně. Možnost nikdy nezvolil žádný respondent.

Obrázek 7: Jak často při své práci nebo studiu přicházíte do styku s databázemi obsahujícími citlivé osobní údaje?



V páté otázce byli respondenti dotazováni jak by celkově ohodnotili úroveň ochrany citlivých údajů v databázích, se kterými se setkávají.

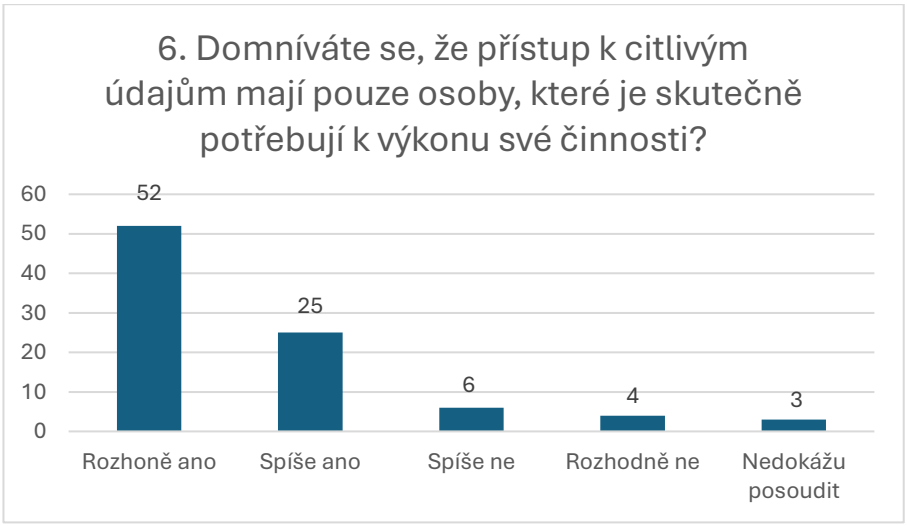
45 respondentů (50 %) ohodnotilo úroveň ochrany jako velmi vysokou, 25 respondentů (27,8 %) ji ohodnotilo jako spíše vysokou, 11 respondentů (12.2 %) ji označilo za průměrnou, negativní hodnocení udělilo 9 respondentů (10 %).

Obrázek 8: Jak byste celkově ohodnotil/a úroveň ochrany citlivých údajů v databázích, se kterými se setkáváte?

V šesté otázce byli respondenti dotazováni zdali se domnívají, že přístup k citlivým údajům mají pouze osoby, které je skutečně potřebují k výkonu své činnosti.

52 respondentů (57,8 %) se domnívá, že rozhodně ano, 25 respondentů (27,8 %) označilo spíše ano, 6 respondentů (6,7 %) si myslí, že spíše ne, 4 respondenti (4,4 %) uvedlo rozhodně ne. 3 respondenti (3,3 %) nedokázalo posoudit.

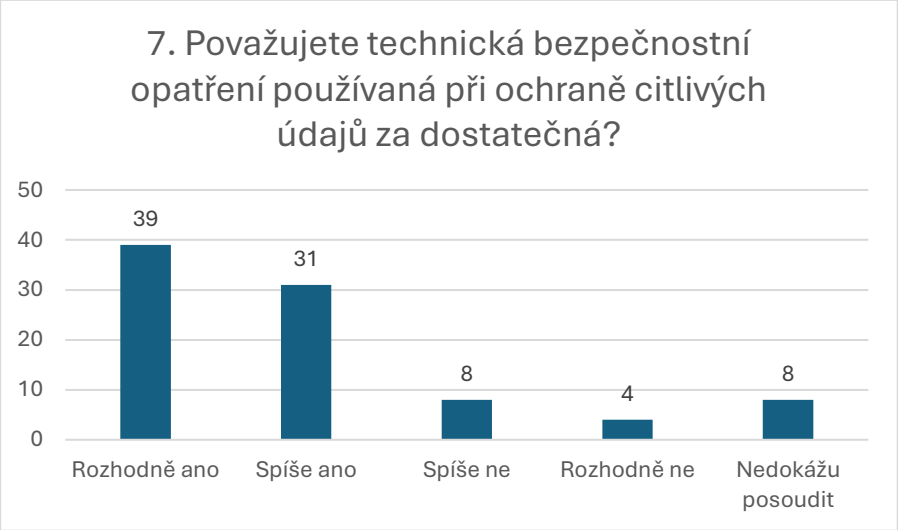
Obrázek 8: Domníváte se, že přístup k citlivým údajům mají pouze osoby, které je skutečně potřebují k výkonu své činnosti?



V sedmé otázce byli respondenti dotazováni zdali považují technická bezpečnostní opatření používaná při ochraně citlivých údajů za dostatečná.

39 respondentů (43,3 %) se domnívá, že rozhodně ano, 31 respondentů (34,4 %) označilo spíše ano, 8 respondentů (8,9 %) si myslí, že spíše ne, 4 respondenti (4,4 %) uvedlo rozhodně ne. 8 respondentů (8,9 %) nedokázalo posoudit.

Obrázek 9: Považujete technická bezpečnostní opatření používaná při ochraně citlivých údajů za dostatečná?



V osmé otázce byli respondenti dotazováni zdali považují organizační opatření, například interní pravidla, kontrolu přístupů nebo školení zaměstnanců, za dostatečná.

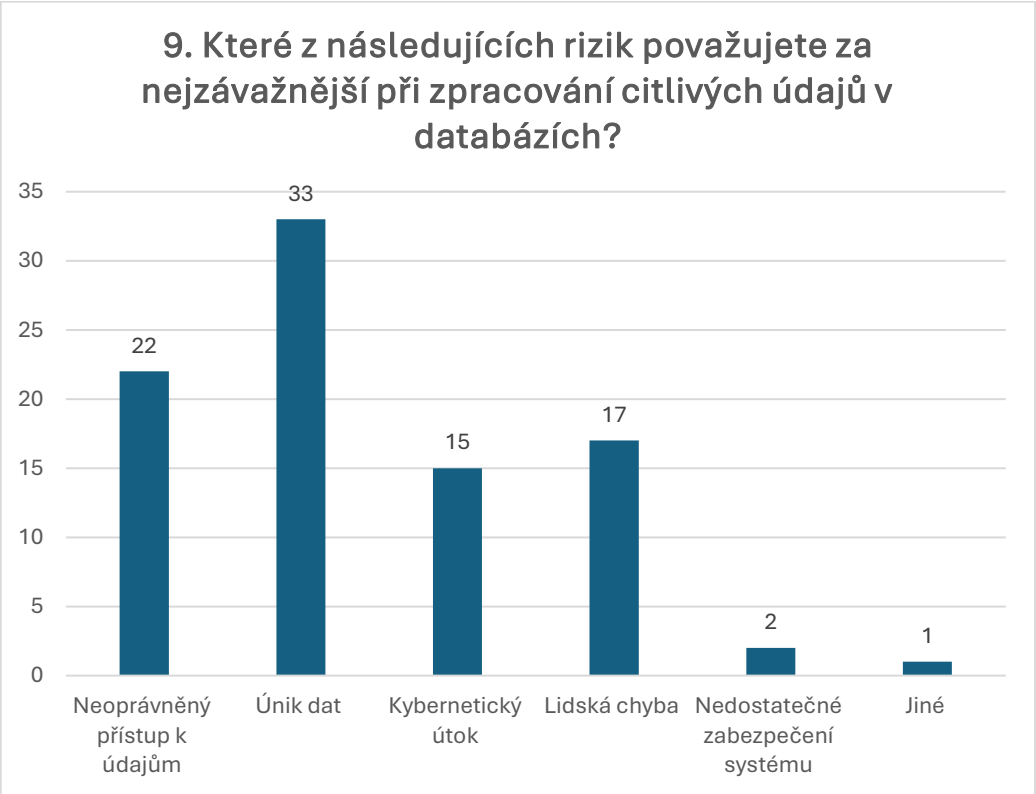
12 respondentů (13,3 %) se domnívá, že rozhodně ano, 43 respondentů (47,8 %) označilo spíše ano, 20 respondentů (22,2 %) si myslí, že spíše ne, 12 respondentů (13,3 %) uvedlo rozhodně ne. 3 respondenti (3,3 %) nedokázalo posoudit.

Obrázek 101: Považujete organizační opatření, například interní pravidla, kontrolu přístupů nebo školení zaměstnanců, za dostatečná?

Devátá otázka se zaměřila na nejzávažnější rizika, spojené se zpracováním citlivých údajů v databázích.

Nejvíce respondentů 33 (36,7 %) označilo za nejvážnější riziko únik dat, 22 respondentů (24,4 %) považuje za nejzávažnější riziko neoprávněného přístupu k údajům, 17 respondentů (18,9 %) připustilo možnost lidského pochybení, 15 respondentů (16,7 %) se obává kybernetického útoku, další možnosti zvolili pouze 3 (3,3 %) oslovení.

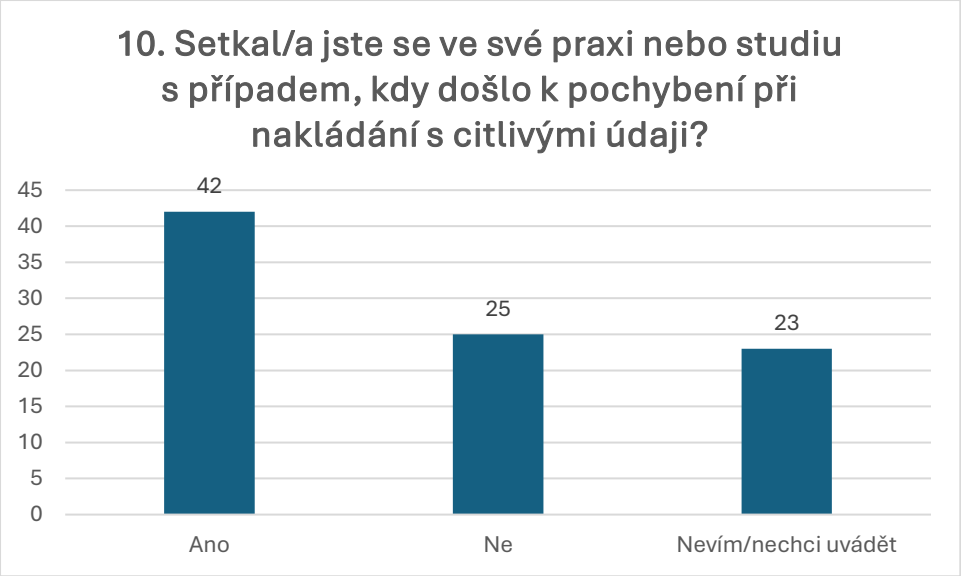
Obrázek 11: Které z následujících rizik považujete za nejzávažnější při zpracování citlivých údajů v databázích?



V desáté a jedenácté otázce byli respondenti dotazováni zdali se setkali ve své praxi nebo studiu s případem, kdy došlo k pochybení při nakládání s citlivými údaji, kdy jedenáctá otázka se týkala pouze respondentů, kteří odpověděli na otázku deset kladně.

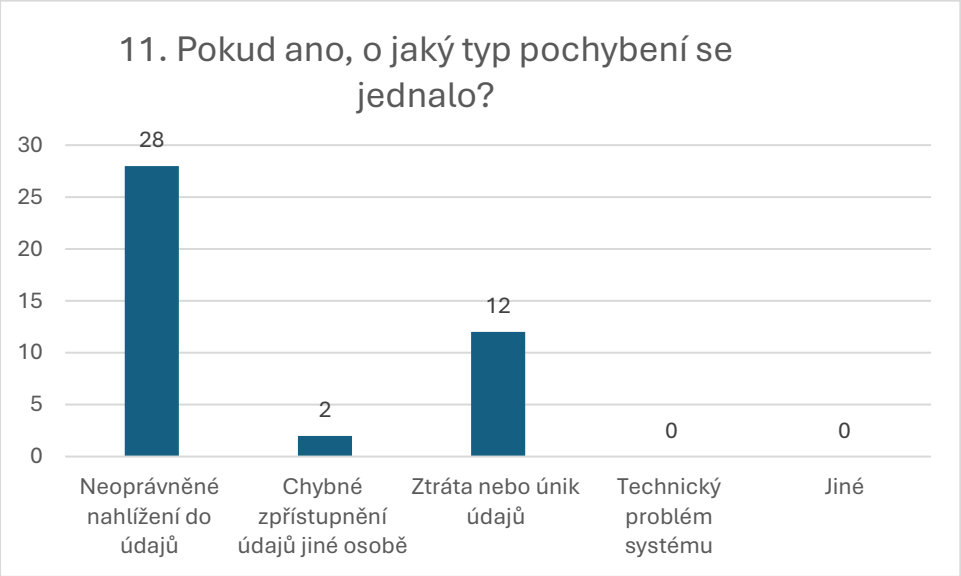
42 respondentů (46,7 %) odpovědělo kladně, 25 respondentů (27,8 %) se s pochybením nesetkalo a 23 respondentů (25,6 %) neodpovědělo.

Obrázek 12: Setkal/a jste se ve své praxi nebo studiu s případem, kdy došlo k pochybení při nakládání s citlivými údaji?



Otázku číslo jedenáct tedy zodpovědělo 42 respondentů, kdy 28 z nich (66,7 %), označilo neoprávněné nahlížení do údajů, 12 respondentů (28,6 %) zvolilo ztrátu nebo únik údajů, a 2 respondenti (4,8 %) se setkalo s chybným zpřístupněním údajů jiné osobě.

Obrázek 134: Pokud ano, o jaký typ pochybení se jednalo?

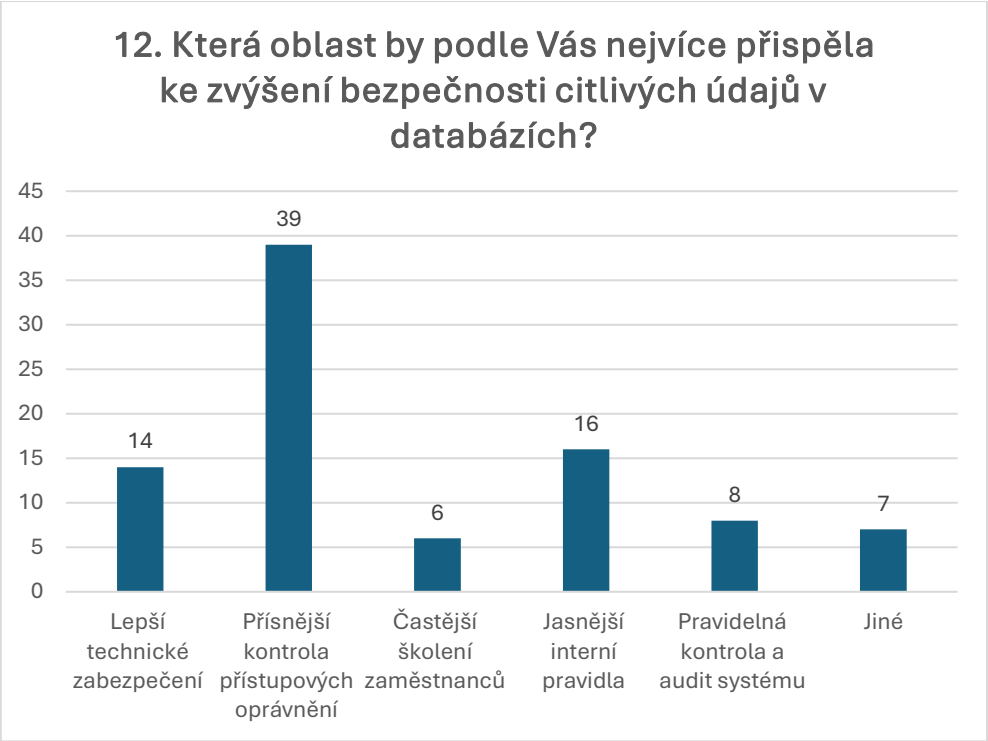


Dvanáctá otázka se zaměřila na oblast, která by nejvíce přispěla ke zvýšení bezpečnosti citlivých údajů v databázích.

39 respondentů (43,3 %) by zpřísnilo kontrolu přístupových oprávnění, 16 respondentů (17,8 %) by určilo jasnější interní pravidla, 14 respondentů (15,6 %) by zlepšilo technické zabezpečení, 8 respondentů (8,9 %) by provádělo pravidelnou

kontrolu a audit systému, 7 respondentů (7,8 %) se domnívá, že by řešení bylo v jiném opatření a 6 respondentů (6,7 %) se domnívá, že řešení se nachází v častějším školení zaměstnanců.

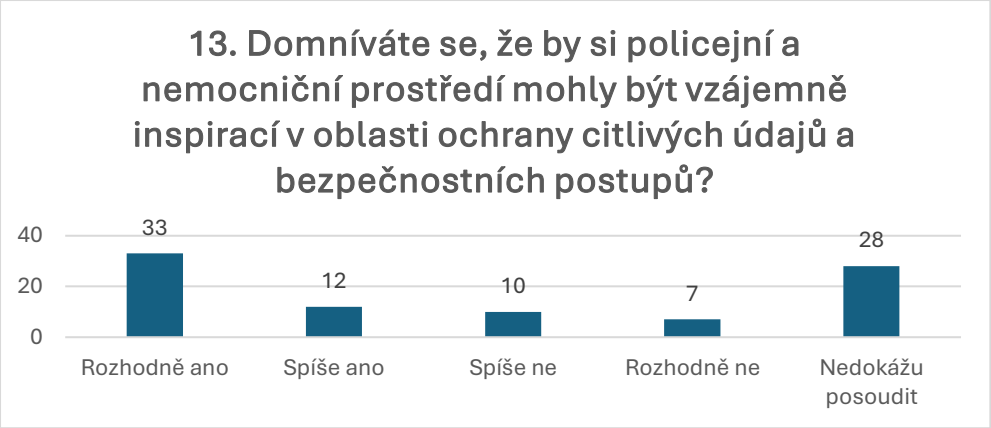
Obrázek 14: Která oblast by podle Vás nejvíce přispěla ke zvýšení bezpečnosti citlivých údajů v databázích?



Ve třínácté otázce byli respondenti dotazováni zdali se domnívají, že by si policejní a nemocniční prostředí mohly být vzájemně inspirací v oblasti ochrany citlivých údajů a bezpečnostních postupů?

33 respondentů (36,7 %) se domnívá, že rozhodně ano, 12 respondentů (13,3 %) označilo spíše ano, 10 respondentů (11,1 %) si myslí, že spíše ne, 7 respondenti (7,8 %) uvedlo rozhodně ne. 28 respondentů (31,1 %) nedokázalo posoudit.

Obrázek 15: Domníváte se, že by si policejní a nemocniční prostředí mohly být vzájemně inspirací v oblasti ochrany citlivých údajů a bezpečnostních postupů?



7.9 Řešení a výsledky

V této kapitole jsou vyhodnoceny hypotézy, které byly stanoveny v bodě 7.6.

Hypotéza 1: Ve většině případů se respondenti domnívají, že přístup k citlivým údajům mají pouze osoby, které je skutečně potřebují k výkonu své činnosti.

Tuto hypotézu lze vyhodnotit pomocí otázky číslo 6. Kladnou odpověď (rozhodně ano a spíše ano) zvolilo 77 respondentů (85,6 %). Tato hypotéza tedy byla potvrzena.

Hypotéza 2: Většina respondentů se domnívá, že ke zvýšení bezpečnosti citlivých údajů by nejvíce přispěla přísnější kontrola přístupových oprávnění a jasnější interní pravidla.

Tuto hypotézu lze vyhodnotit pomocí otázky číslo 12. 39 respondentů (43,3 %) by zpřísnilo kontrolu přístupových oprávnění, 16 respondentů (17,8 %) by určilo jasnější interní pravidla, tedy 55 respondentů (61,1 %) se domnívá tyto 2 atributy by napomohly ke zvýšení bezpečnosti citlivých údajů v databázích. Tato hypotéza je tedy potvrzena.

Hypotéza 3: Za nejzávažnější riziko při zpracování citlivých údajů v databázích považují respondenti nejčastěji neoprávněný přístup k údajům.

K vyhodnocení této hypotézy sloužila otázka číslo 9. Nejvíce respondentů 33 (36,7 %) označilo za nejvážnější riziko únik dat, 22 respondentů (24,4 %) považuje za nejzávažnější riziko neoprávněného přístupu k údajům. Tato hypotéza tedy byla vyvrácena.

Závěr

Cílem bakalářské práce bylo porovnat přístupy k ochraně citlivých osobních údajů v policejních a nemocničních databázích, poukázat na jejich silné a slabé stránky a současně zjistit, v čem se mohou tato dvě prostředí vzájemně inspirovat. Součástí práce bylo také dotazníkové šetření mezi pracovníky Policie České republiky a pracovníky nemocničních zařízení, jehož úkolem bylo doplnit teoretická východiska o pohled z praxe.

Na základě zpracovaných poznatků lze konstatovat, že stanovený cíl práce byl splněn. Teoretická část ukázala, že policejní a nemocniční databáze fungují v odlišném právním i praktickém prostředí, jejich společným znakem je však práce s velmi citlivými osobními údaji, u nichž je nezbytné zajistit vysokou úroveň ochrany. Rozdíly mezi oběma oblastmi vyplývají zejména z účelu, pro který jsou údaje zpracovávány, z okruhu oprávněných osob i z povahy samotných uchovávaných informací. Zatímco v případě nemocničních databází je v popředí především zajištění zdravotní péče a návaznost na zdravotnickou dokumentaci, policejní databáze plní úkoly spojené s ochranou bezpečnosti, veřejného pořádku a odhalováním protiprávního jednání.

Práce zároveň potvrdila, že ochranu citlivých údajů nelze chápat pouze jako otázku právní úpravy nebo technického zabezpečení. Významnou roli zde hraje také každodenní praxe, vnitřní pravidla organizace, kontrola přístupových oprávnění a odpovědný přístup osob, které s údaji pracují. Právě v této rovině se ukazuje, že i dobře nastavený systém může být oslaben lidským pochybením, nedostatečnou kontrolou nebo nejasně vymezenými pravidly.

Za důležitý poznatek považuji i to, že mezi policejním a nemocničním prostředím lze nalézt nejen rozdíly, ale i určité společné principy. V obou případech je nezbytné, aby přístup k údajům měly pouze oprávněné osoby, aby bylo možné kontrolovat, kdo s údaji pracoval, a aby byla přijímána odpovídající technická i organizační opatření. Současně se ukazuje, že ochrana citlivých údajů musí být vnímána jako průběžný proces, nikoli jako jednorázově nastavené opatření.

Výsledky dotazníkového šetření teoretická východiska v zásadě potvrdily. Většina respondentů uvedla, že se ve své praxi setkává s databázemi obsahujícími citlivé

osobní údaje pravidelně, často i každodenně. Z odpovědí dále vyplynulo, že respondenti hodnotí současnou úroveň ochrany těchto údajů spíše pozitivně, zároveň však vnímají i prostor pro další zlepšení. Jako nejzávažnější rizika byly označovány zejména únik dat, neoprávněný přístup a lidské pochybení. Tato zjištění potvrzují, že ochrana citlivých údajů je v praxi stále velmi aktuálním tématem a že riziko nespočívá pouze v technické stránce systému, ale i v samotném způsobu jeho používání.

Za významné lze považovat také to, že respondenti spatřují možnost zlepšení zejména v důslednější kontrole přístupových oprávnění, v jasněji nastavených interních pravidlech a v prevenci bezpečnostních incidentů. Právě tato oblast se podle mého názoru jeví jako jedna z nejdůležitějších, protože spojuje právní požadavky s každodenním fungováním konkrétních pracovišť. Lze tedy říci, že účinná ochrana citlivých osobních údajů nestojí pouze na existenci právních předpisů, ale především na tom, jak jsou tato pravidla skutečně uplatňována v praxi.

Přínos bakalářské práce spatřuji především v propojení teoretického a praktického pohledu na problematiku ochrany citlivých osobních údajů ve dvou významných profesních oblastech. Výzkumná sonda umožnila doplnit teoretická východiska o konkrétní zkušenosti a názory respondentů z praxe, a přispěla tak k lepšímu pochopení toho, jak jsou otázky ochrany citlivých údajů, souvisejících rizik a bezpečnostních opatření vnímány přímo osobami, které s těmito databázemi pracují. Práce tak ukazuje, že ačkoli policejní a nemocniční databáze sledují odlišné cíle, požadavky na odpovědné nakládání s údaji, jejich zabezpečení a kontrolu přístupu jsou v mnohém srovnatelné. Přínos práce lze spatřovat i v tom, že upozorňuje na význam lidského faktoru, který bývá v souvislosti s ochranou dat někdy podceňován, přestože právě ten může být pro bezpečnost systému rozhodující.

Současně je však třeba uvést, že provedená výzkumná sonda měla orientační charakter, a její výsledky proto nelze bez dalšího zobecňovat na celé prostředí Policie České republiky nebo všech zdravotnických zařízení. Přesto se domnívám, že zjištěné poznatky mají určitou vypovídací hodnotu a mohou být užitečné pro další úvahy o tom, jak ochranu citlivých osobních údajů v praxi dále posilovat.

Za hlavní význam práce lze považovat to, že poukazuje na potřebu vnímat ochranu citlivých osobních údajů komplexně, tedy nejen jako právní povinnost, ale i jako důležitou součást fungování policejního a zdravotnického prostředí.

Seznam použitých zdrojů

Literární zdroje

1. CONNELLY KOHUTOVÁ, Radka. *Databáze ve věku informační společnosti a jejich právní ochrana*. Praha: C. H. Beck, 2013, 207 s. ISBN 978-80-7400-493-3.
2. HABICH, Lukáš; STEIN, Petr; HLAVÁČKOVÁ, Kateřina. *Policejní právo.* Praha: Wolters Kluwer ČR, 2025. 184 s. ISBN 978-80-7676-606-8.
3. JÄGER, Petr; BAUER, Jaroslav; KŘÍŽKA, Vít; MATEJKA, Ján; MATES, Pavel a POLÁK, Michal. *Svobodný přístup k informacím. Zákon č. 106/1999 Sb.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2025, 258 s. ISBN 978-80-7380-964-5.
4. JANEČKOVÁ, Eva. *GDPR. Praktická příručka implementace.* Praha: Wolters Kluwer ČR, 2018. 119 s. ISBN 978-80-7552-248-1.
5. KREJČÍ, Jindřich; LEONTIYEVA, Yana, eds. *Cesty k datům: zdroje a management sociálněvědních dat v České republice.* Praha: Sociologické nakladatelství (SLON), 2012. 469 s. ISBN 978-80-7419-111-4.
6. MELOTÍKOVÁ, Petra. *Ochrana osobních údajů v rámci veřejné správy.* Praha: Leges, 2018. 150 s. ISBN 978-80-7502-275-2.
7. MELOTÍKOVÁ, Petra. Osobní údaje v kontextu GDPR. Praha: Leges, 2020. 139 s. ISBN 978-80-7502-507-4.
8. NAVRÁTIL, Jiří a kol. *GDPR pro praxi.* Plzeň: Aleš Čeněk, 2018. 339 s. ISBN 978-80-7380-689-7.
9. NULÍČEK, Michal; DONÁT, Josef; NONNEMANN, František; LICHNOVSKÝ, Bohuslav; TOMÍŠEK, Jan. *GDPR. Obecné nařízení o ochraně osobních údajů. Praktický komentář.* Praha: Wolters Kluwer ČR, 2017. 525 s. ISBN 978-80-7552-765-3.
10. PFLEEGER, Charles P.; PFLEEGER, Shari Lawrence a MARGULIES, Jonathan. *Security in Computing*. 5th ed. Boston: Pearson, 2015, 800 s. ISBN 978-0-13-408504-3.
11. SILBERSCHATZ, Avi; KORTH, Henry F.; SUDARSHAN, S. *Database System Concepts*. 7th ed. New York: McGraw-Hill Education, 2019, 1376 s. ISBN 978-00-7802-215-9.
12. SODOMKA, Petr; KLČOVÁ, Hana. *Informační systémy v podnikové praxi*. Brno: Computer Press, 2010. 501 s. ISBN 978-80-251-2878-7.

13. STAŇKOVÁ, Lucie. *GDPR snadno a přehledně.* Praha: Mladá fronta, 2018. 366 s. ISBN 978-80-204-5108-8.
14. ŠEBESTA, Patrik. *Zákon o obecní policii: Komentář.* Praha: Wolters Kluwer ČR, 2018. 279 s. ISBN 978-80-7552-455-3.
15. ŠTEINBACH, Miroslav; ŠLESINGER, René; ZIMMERMANN, Miroslav; BÍLEK, Milan; HLAVÁČKOVÁ, Kateřina. *Zákon o Policii České republiky: Komentář.* Praha: Wolters Kluwer ČR, 2019. 280 s. ISBN 978-80-7598-193-6.

Elektronické zdroje

1. KUTÍNOVÁ, Miluše a Jiří MACUR. Informační technologie a systémová analýza: studijní opory pro studijní programy s kombinovanou formou studia [online]. Brno: Vysoké učení technické v Brně, 2006 [cit. 26. 3. 2026]. Dostupné z WWW: https://www.fce.vutbr.cz/aiu/macur.j/bu04/BU04_M01.pdf.
2. NÁRODNÍ CENTRUM ELEKTRONICKÉHO ZDRAVOTNICTVÍ. Národní strategie elektronického zdravotnictví [online]. Praha: Ministerstvo zdravotnictví České republiky, bez data [cit. 26. 3. 2026]. Dostupné z WWW: https://ncez.mzcr.cz/cs/narodni-strategie-elektronickeho-zdravotnictvi/narodni-strategie-elektronickeho-zdravotnictvi
3. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Národní strategie kybernetické bezpečnosti 2026–2030 [online]. Brno: NÚKIB, 2025 [cit. 2026-03-25]. Dostupné z WWW: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2026-2030.pdf.
4. POLICIE ČESKÉ REPUBLIKY. Zpracování osobních údajů Policií České republiky [online]. Praha: Policie České republiky, [cit. 26. 3. 2026]. Dostupné z WWW: https://policie.gov.cz/clanek/zpracovani-osobnich-udaju-policii-ceske-republiky.aspx

Legislativní dokumenty

1. ČESKO. Zákon č. 110 ze dne 12. března 2019 o zpracování osobních údajů. In: Sbírka zákonů, Česká republika. 2019, částka 47, s. 890–906. Dostupné z WWW: <https://www.psp.cz/sqw/sbirka.sqw?cz=110&r=2019>. ISSN 1211-1244.

2. ČESKO. Zákon č. 273 ze dne 17. července 2008 o Policii České republiky. In: Sbírka zákonů, Česká republika. 2008, částka 91, s. 4085–4156. Dostupné z WWW: <https://mv.gov.cz/soubor/sb091-08-pdf.aspx>. ISSN 1211-1244.
3. ČESKO. Zákon č. 372 ze dne 6. listopadu 2011 o zdravotních službách a podmínkách jejich poskytování (zákon o zdravotních službách). In: Sbírka zákonů, Česká republika. 2011, částka 131, s. 4729–4904. Dostupné z WWW: <https://www.psp.cz/sqw/sbirka.sqw?cz=372&r=2011>. ISSN 1211-1244.
4. ČESKO. Zákon č. 325 ze dne 18. srpna 2021 o elektronizaci zdravotnictví. In: Sbírka zákonů, Česká republika. 2021, částka 143, s. 3868–3883. Dostupné z WWW: <https://www.psp.cz/sqw/sbirka.sqw?cz=325&r=2021>. ISSN 1211-1244.
5. ČESKO. MINISTERSTVO ZDRAVOTNICTVÍ. Vyhláška č. 444 ze dne 19. prosince 2024 o zdravotnické dokumentaci. In: Sbírka zákonů a mezinárodních smluv, Česká republika. 2024, akt č. 444/2024 Sb. Dostupné z WWW: <https://www.e-sbirka.cz/sb/2024/444>.ISSN 3029-5092.
6. ČESKO (ČESKOSLOVENSKO). Zákon České národní rady č. 553 ze dne 6. prosince 1991 o obecní policii. In: Sbírka zákonů České a Slovenské Federativní Republiky. 1991, částka 104, s. 2739–2742. Dostupné z WWW: <https://www.psp.cz/sqw/sbirka.sqw?cz=553&r=1991>. ISSN 1210-0005.

Ostatní zdroje

Kromě výše uvedených zdrojů byly při zpracování bakalářské práce využity následující materiály:

databáze Automatizovaného rozpočtového informačního systému MF ČR

Seznam obrázků

Obrázek 29: Domníváte se, že by si policejní a nemocniční prostředí mohly být vzájemně inspirací v oblasti ochrany citlivých údajů a bezpečnostních postupů?

Seznam zkratek

DBMS – systém řízení báze dat

ETŘ – evidence trestního řízení

GDPR – General Data Protection Regulation

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

NoSQL – Not Only SQL

PNR – Passenger Name Record

RDBMS – relační databázový systém

SQL – Structured Query Language

UBYPORT – aplikace Policie České republiky pro hlášení ubytovaných osob

Seznam příloh

Příloha I. - Výzkumná sonda (dotazník)

Dostupné z:

https://forms.office.com/Pages/ResponsePage.aspx?id=mLYPYK6XOkCoGHPLXvEy54I3bKBStzFMkTudDdwKuYdUOERXQjhDN0NKSUtXVE1JOThSMFYyQ0lGUS4u

Příloha č. I - výzkumná sonda (dotazník)

1. Věk:

☐ 18-25

☐ 26-35

☐ 36-45

☐ 46-55

☐ 56 a více

2. Pohlaví:

☐ Muž

☐ Žena

3. V jakém prostředí se nejčastěji setkáváte s databázemi obsahujícími citlivé osobní údaje?

☐ policejní prostředí

☐ nemocniční / zdravotnické prostředí

4. Jak často při své práci nebo studiu přicházíte do styku s databázemi obsahujícími citlivé osobní údaje?

☐ denně

☐ několikrát týdně

☐ několikrát měsíčně

☐ výjimečně

☐ nikdy

5. Jak byste celkově ohodnotil/a úroveň ochrany citlivých údajů v databázích, se kterými se setkáváte?

☐ velmi vysoká

☐ spíše vysoká

☐ průměrná

☐ spíše nízká

☐ velmi nízká

6. Domníváte se, že přístup k citlivým údajům mají pouze osoby, které je skutečně potřebují k výkonu své činnosti?

☐ rozhodně ano

☐ spíše ano

☐ spíše ne

☐ rozhodně ne

☐ nedokážu posoudit

7. Považujete technická bezpečnostní opatření používaná při ochraně citlivých údajů za dostatečná?

☐ rozhodně ano

☐ spíše ano

☐ spíše ne

☐ rozhodně ne

☐ nedokážu posoudit

8. Považujete organizační opatření, například interní pravidla, kontrolu přístupů nebo školení zaměstnanců, za dostatečná?

☐ rozhodně ano

☐ spíše ano

☐ spíše ne

☐ rozhodně ne

☐ nedokážu posoudit

9. Které z následujících rizik považujete za nejzávažnější při zpracování citlivých údajů v databázích?

☐ neoprávněný přístup k údajům

☐ únik dat

☐ kybernetický útok

☐ lidská chyba

☐ nedostatečné zabezpečení systému

☐ jiné

10. Setkal/a jste se ve své praxi nebo studiu s případem, kdy došlo k pochybení při nakládání s citlivými údaji?

☐ ano

☐ ne

☐ nevím / nechci uvést

11. Pokud ano, o jaký typ pochybení se jednalo?

☐ neoprávněné nahlížení do údajů

☐ chybné zpřístupnění údajů jiné osobě

☐ ztráta nebo únik údajů

☐ technický problém systému

☐ jiné

12. Která oblast by podle Vás nejvíce přispěla ke zvýšení bezpečnosti citlivých údajů v databázích?

☐ lepší technické zabezpečení

☐ přísnější kontrola přístupových oprávnění

☐ častější školení zaměstnanců

☐ jasnější interní pravidla

☐ pravidelná kontrola a audit systému

☐ jiné

13. Domníváte se, že by si policejní a nemocniční prostředí mohly být vzájemně inspirací v oblasti ochrany citlivých údajů a bezpečnostních postupů?

☐ rozhodně ano

☐ spíše ano

☐ spíše ne

☐ rozhodně ne

☐ nedokážu posoudit