

Inteligentní digitální systémy: zpráva o srovnávací případové studii

Shrnutí

Autoři: Paweł Hess, Aleksandra Skoczylas, Joanna Smętek, Ewelina Wołosik, Andrzej Zurawski

Vedení projektu: Annick Starren, Ioannis Anyfantis – Evropská agentura pro bezpečnost a ochranu zdraví při práci (EU-OSHA)

Tuto zprávu zadala k vypracování Evropská agentura pro bezpečnost a ochranu zdraví při práci (EU-OSHA). Její obsah, včetně všech vyjádřených názorů a závěrů, představuje výhradně stanovisko autorů a nemusí nutně odrážet postoj agentury EU-OSHA.

Ani Evropská agentura pro bezpečnost a ochranu zdraví při práci, ani žádná jiná osoba jednající jménem agentury není odpovědná za případné využití těchto informací.

© Evropská agentura pro bezpečnost a ochranu zdraví při práci, 2024

Reprodukce povolena s uvedením zdroje.

Pro každé použití nebo reprodukci fotografií či jiných materiálů, na které se nevztahují autorská práva Evropské agentury pro bezpečnost a ochranu zdraví při práci, je nutno získat souhlas přímo od držitelů autorských práv. Pokud konkrétní obsah zobrazuje identifikovatelné soukromé osoby nebo obsahuje díla třetích stran, musíte si zajistit zvláštní práva také k těmto částem.

1 Úvod

Jedná se o souhrnnou zprávu o závěrečné srovnávací komplexní zprávě vypracované v rámci projektu agentury EU-OSHA „Smart digital systems for improving worker safety and health – overview of

research and practices“¹ (Inteligentní digitální systémy pro zlepšení bezpečnosti a ochrany zdraví pracovníků – přehled výzkumu a praxe), která vychází ze zjištění uvedených v této zprávě.

Inteligentní digitální systémy a technologie se začínají objevovat na pracovištích v EU a přetvářejí pracovní prostředí pro zaměstnance i zaměstnavatele. Inovace, jako jsou chytrá nositelná zařízení, exoskelety, umělá inteligence (AI), strojové učení (ML), internet věcí (IoT), virtuální a rozšířená realita (VR a AR), přináší mimo jiné nové možnosti prevence a reakce na rizika na pracovišti.

V rámci souhrnného programu agentury EU-OSHA pro bezpečnost a ochranu zdraví při práci (BOZP) (2020–2023)² agentura EU-OSHA zkoumá výzvy a příležitosti, jež přináší inteligentní digitální nástroje a monitorovací systémy, pokud jde o zlepšení bezpečnosti a ochrany zdraví pracovníků. Tyto systémy využívají digitální technologie ke sběru a analýze dat s cílem identifikovat a vyhodnocovat rizika, předcházet škodám a/nebo je minimalizovat a podporovat BOZP.³ Agentura EU-OSHA rozdělila tyto systémy do dvou kategorií: proaktivní (preventivní) a reaktivní, i když uznává, že se tyto dvě kategorie mohou překrývat.⁴ Agentura EU-OSHA dále poskytla přehled rizik a příležitostí spojených s těmito systémy⁵ a prozkoumala zdroje na pracovišti, které by mohly zajistit jejich bezpečné a zdravé používání.⁶

Agentura EU-OSHA vypracovala řadu případových studií s cílem prozkoumat praktické zavádění inteligentních digitálních nástrojů a nových systémů pro monitorování BOZP za účelem zlepšení bezpečnosti a ochrany zdraví pracovníků.

Případové studie se tedy zabývají aspekty týkajícími se vývojové fáze a fáze zavádění⁷. Ve všech případových studiích byly s ohledem na typ případové studie zohledněny aspekty BOZP, včetně zapojení pracovníků. Dále se všechny případové studie zabývají možnými hnacími silami, překážkami a faktory úspěchu pro bezpečné a účinné zavádění.

Pro každou případovou studii byl ve spolupráci se společnostmi, na niž se studie zaměřuje, vypracován na míru uzpůsobený protokol o výzkumu, aby se zajistilo, že byly shromážděny všechny relevantní informace. Mezi metody sběru dat patří sekundární výzkum, individuální rozhovory, diskuse v ohniskových skupinách a kontextualizační rozhovory.

Podrobná zjištění z případových studií jsou uvedena odděleně v samostatných zprávách o případových studiích. Úplná srovnávací perspektiva je k dispozici v (samostatné) srovnávací souhrnné zprávě.

2 Přehled případových studií

V případových studiích jsou uvedeny příklady používání **inteligentních digitálních systémů a systémů pro monitorování BOZP**⁸. Definice systémů pro monitorování BOZP (viz níže) byla pro tuto studii přijata na základě stávajících definic systémů pro monitorování BOZP a dalších monitorovacích systémů a shromážděných důkazů o jejich typech a účelech.

¹ Zpráva je k dispozici na adrese: <https://osha.europa.eu/en/publications/smart-digital-systems-improving-worker-safety-and-health-overview-research-and-practices>.

² Pro více informací viz: osha.europa.eu (n.d.) Digitalizace práce. <https://osha.europa.eu/en/themes/digitalisation-work>

³ EU-OSHA (2023). Inteligentní digitální systémy pro monitorování bezpečnosti a ochrany zdraví při práci: využití a související výzvy.

<https://osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-uses-and-challenges>

⁴ Tamtéž.

⁵ Tamtéž.

⁶ EU-OSHA (2023). Inteligentní digitální systémy pro monitorování bezpečnosti a ochrany zdraví při práci: zdroje na pracovišti pro jejich navrhování, zavádění a používání.

<https://osha.europa.eu/en/publications/smart-digital-monitoring-systems-occupational-safety-and-health-workplace-resources-design-implementation-and-use>

⁷ V předchozích publikacích agentury EU-OSHA byly použity pojmy „osoba zodpovědná za návrh“, „osoba zodpovědná za zavádění“ a „uživatel systému“. Je tomu tak proto, že v době přípravy těchto publikací (2021) nebyl ještě Evropským parlamentem přijat akt o umělé inteligenci (nařízení (EU) 2024/1689). Vzhledem k tomu, že akt o umělé inteligenci je nyní oficiálně přijat, budou v této zprávě z důvodu jasnosti a jednotnosti používány pojmy „vývoje“ a „zavádějící subjekt“.

⁸ Tento pojem se používá zaměnitelně s pojmy „inteligentní monitorovací systémy“ a „inteligentní digitální systémy“.

„Nové systémy pro monitorování BOZP využívají digitální technologie ke shromažďování a analýze údajů za účelem identifikace a hodnocení rizik, prevence a/nebo minimalizace škod a podpory bezpečnosti a ochrany zdraví při práci.“⁹

Výše uvedená definice vystihuje rozmanitost **technologií**, které jsou začleněny do systémů pro monitorování, jež pomáhají zlepšovat BOZP na dnešních pracovištích. Z devíti vypracovaných případových studií stojí za povšimnutí to, jak lze různé technologie kombinovat a integrovat, aby se zlepšilo odhalování, hodnocení a řízení rizik pro účely BOZP. Ve všech případech se nové technologie používají pro specifické funkce, jejichž výsledkem jsou integrované, inteligentní digitální systémy.

Kromě toho je v případových studiích doloženo uplatnění dvou přístupů, jež využívají inteligentní digitální systémy v oblasti BOZP, jak již bylo uvedeno výše:

- prvním z nich je **proaktivní** přístup, který se snaží o prevenci újmy a v širším ohledu o podporu zdraví,
- a druhým je **reaktivní** přístup, který se zaměřuje na reakce na úrazy či nehody a na mimořádné události.

Nejprve byl sestaven dlouhý seznam 15 možných příkladů (potenciálních případových studií), na jehož základě bylo vypracováno 9 případových studií. Většina případových studií byla provedena v Evropě (Francii, Německu, Irsku, Španělsku a Spojeném království) a některé mimo Evropu (v Austrálii, Spojeném království, Spojených státech). Studie se zabývají také vývojáři (rovněž označovanými jako poskytovatelé) i uživateli (označovanými také jako zavádějící subjekty) systémů. Pokud jde o technologie/použití, jedná se o nositelná zařízení navržená pro lepší ergonomii, například inteligentní vložky do obuvi pro ochranu (osamocených) pracovníků (lone worker), sběr dat v reálném čase pro účinné řízení bezpečnosti nebo pro sledování rizik pro životní prostředí a únavy pracovníků, umělou inteligenci (AI) a počítačové vidění pro předvídání rizik pracovníků a zlepšení podávání zpráv o bezpečnosti, přenosné detektory plynů a zařízení typu chytré sklo pro účely provádění hodnocení a auditů BOZP na dálku.

Škála rizik, o nichž se pojednává v případových studiích, zahrnuje:

- individuální a kolektivní škodlivé expozice a environmentální úrovně,
- expozice ergonomickým rizikům,
- rizika spojená se závodem a prostory,
- nebezpečné chování pracovníků,
- rizika související s dobrými životními podmínkami a únavou,
- psychosociální rizika.

3 Proces zavádění: překážky a faktory usnadňující zavádění

Na základě praktických zkušeností z případových studií byla identifikována řada motivačních faktorů a cílů pro zavádění systémů, jakož i poznatků ze zavádění systémů – překážek a faktorů usnadňujících zavádění.

Primární hnací silou pro zavádění inteligentních digitálních systémů je snaha zvýšit bezpečnost a ochranu zdraví na pracovišti, a tím mohou systémy pomoci snížit fluktuaci a náklady na odškodnění zaměstnanců. Systémy mohou vykazovat flexibilitu a adaptabilitu a splňovat požadavky na zavádění ergonomických a inovativních řešení v oblasti BOZP. Pandemie covidu-19 vedla k nárůstu využívání systémů pro monitorování BOZP a k většímu zájmu o témata týkající se BOZP obecně. V neposlední

⁹ EU-OSHA – Evropská agentura pro bezpečnost a ochranu zdraví při práci, *Inteligentní digitální systémy pro monitorování bezpečnosti a ochrany zdraví při práci: využití a související výzvy*, 2022. https://osha.europa.eu/sites/default/files/Smart-digital-monitoring-systems-uses-challenges_en.pdf

řadě pak širší osvojování technologií ze strany společností a v každodenním životě pracovníků rovněž přispělo k většímu přijímání inteligentních digitálních systémů.

Inteligentní digitální systémy jsou navrženy tak, aby včas odhalily nebezpečné podmínky nebo chování, lokalizovaly pracovníky v tísňové situaci a zlepšily BOZP. Pro zavedení těchto systémů však existuje několik překážek. Jedna z hlavních překážek souvisí s obavami pracovníků ohledně soukromí a možného zneužití údajů, které mohou být citlivé povahy, což poukazuje na potřebu plné anonymizace údajů. Zavádění inteligentních digitálních systémů souvisí také s velikostí společnosti a odvětvím činnosti, přičemž u modernějších technologií je míra zavádění nižší. Ze shromážděných informací vyplývá, že některé společnosti se zdráhají používat nositelná zařízení, umělou inteligenci a jiné špičkové technologie na pracovišti, např. v důsledku nedostatku informací, krátkodobých investičních nákladů nebo obav z jejich dopadu na pracoviště. Třetí překážka pro provádění BOZP souvisí s nedostatkem digitálních dovedností pracovníků a nedostatečnou infrastrukturou IKT – zejména v malých a středních podnicích – potřebných pro zavádění nových systémů.

Ve studiích se zdůrazňuje, že úzká interakce mezi společnostmi, které danou technologii navrhly, a společnostmi, které ji zavádějí, – poskytovateli a zavádějícími subjekty – a společné chápání potřeb a priorit pracovníků má zásadní význam pro zajištění úspěšného zavedení inteligentního systému. Tato spolupráce je nejzřetelnější během zavádění řešení na místě. Spolupráce ve fázi návrhu a vývoje je méně viditelná, a pokud k ní dojde, obvykle má podobu investice a závazku k prvnímu inovačnímu nápadu společnosti, která je poskytovatelem/navrhovatelem. Spolupráce se obecně skládá z klíčových kroků, které jsou ve všech společnostech podobné: přizpůsobení řešení potřebám zavádějícího/provádějícího subjektu a možnosti vyzkoušení a odborné přípravy.

4 Dopady na BOZP: příležitosti a výzvy

Pokud jde o dopady inteligentních digitálních systémů na BOZP, byla identifikována řada příležitostí a výzev.

Příležitosti

- Technologie v oblasti BOZP otevřely nové **možnosti** pro předcházení úrazům, kolizím, pádům a dalším událostem, které mohou bezprostředně ohrozit zaměstnance nebo jiné osoby (tj. proaktivní přístup k BOZP), často prostřednictvím monitorování v reálném čase a okamžitého varování.
- Bylo prokázáno, že inovativní technologie mají preventivní funkci, pokud jde o širokou škálu rizik pro BOZP. Zejména prediktivní funkce výrazně posilují proaktivní přístup k rizikům v oblasti BOZP. Inteligentní digitální systémy usnadňují včasné reakce na jakékoli události, které nebylo možné předvídat pomocí žádného monitorovacího nástroje. Ze systémového hlediska posílilo přizpůsobení inovativních technologií v oblasti BOZP proaktivní prevenci úrazů tím, že umožnilo získat velmi specifické poznatky o rizicích souvisejících s pracovištěm a pracovníky – zlepšilo sběr a analýzu dat. Poznatky založené na datech mohou vést k lepšímu uspořádání pracoviště, lepší ergonomii, zkvalitnění vzdělávacích programů a lepšímu přidělování zdrojů. Souhrnná data z více zdrojů poskytují komplexní přehled o bezpečnosti a ochraně zdraví na pracovišti a usnadňují informované rozhodování a analýzu trendů.
- Technologie popsané v případových studiích navíc svědčí o výrazném rozšíření chápání BOZP. Místo toho, aby se navrhující subjekty zaměřovaly pouze na prevenci úrazů, zabývají se mnohem širší kategorií dobrých pracovních podmínek pracovníků. Díky těmto systémům mohou mít pracoviště prospěch nejen ze zvýšené bezpečnosti, ale také ze zvýšené spokojenosti s prací nebo lepší efektivity práce. Případové studie rovněž dokládají, že hranice mezi reaktivními a proaktivními technologiemi v oblasti BOZP se do značné míry stírá.
- Pokud jde o příležitosti pro řízení BOZP, jedním z nejvýznamnějších přínosů je schopnost účinněji a účelněji zlepšit ochranu zdraví a bezpečnost. Vynikajícím příkladem je možnost

provádět hodnocení a inspekce na dálku. Některé technologie nabízí možnost provádět je na dálku, aniž by bylo nutné pokaždé dojet na pracoviště, což šetří čas i náklady.

- Data shromážděná prostřednictvím technologií v oblasti BOZP navíc umožňují organizaci procesu BOZP na základě „tvrdých ukazatelů“, které obvykle nejsou v případě tradičních technologií pro monitorování BOZP k dispozici. Tyto údaje rovněž umožňují odborníkům na BOZP zlepšit dodržování veškerých právních předpisů, včetně požadavků na ochranu zdraví a bezpečnost. Inteligentní digitální systémy mohou zlepšit řízení dodržování předpisů tím, že poskytují přesné záznamy a zjednodušují proces auditu poskytováním komplexních a uspořádaných dat. Díky tomu lze zlepšit transparentnost a odpovědnost. Rozsáhlé využívání dat s podporou umělé inteligence a strojového učení pomáhá odborníkům na BOZP lépe pochopit situaci v jejich společnostech. Díky tomu mohou snáze upravit systémy, odbornou přípravu a interní postupy na úrovni podniku za účelem dalšího zlepšení bezpečnosti na pracovišti.
- Je zajímavé, že technologie pro monitorování BOZP umožňují začlenění široké škály pracovníků do procesů BOZP a vytvářejí příležitost pro větší inkluzivnost postupů v oblasti bezpečnosti a ochrany zdraví, které jsou přístupné pracovníkům, ať už jsou jakéhokoliv pohlaví, mají jakoukoliv velikost těla a jakékoliv právní postavení z hlediska migrace.
- V neposlední řadě pak díky inteligentním digitálním systémům vykazují pracovníci vyšší výkonnost a větší povědomí o bezpečnosti a ochraně zdraví. Přestože se většina těchto technologií stále nachází v raných fázích zavádění, již existují přesvědčivé důkazy, že po jejich zavedení se výrazně snížil počet úrazů a zranění. Pracovníci navíc mají prospěch ze změny paradigmatu v oblasti BOZP, již tyto technologie podporují. Vzhledem k tomu, že „dobré pracovní podmínky“ jsou vnímány jako širší pojem než „předcházení úrazům“, lze pozorovat pozitivní dopady na BOZP, a to zejména s ohledem na dlouhodobou perspektivu. Lepší informovanost o BOZP se navíc v dlouhodobém horizontu promítá do zlepšení zdraví a bezpečnosti. Pracovníci se více zajímají o vlastní bezpečnost, což vede ke kultuře proaktivního bezpečnostního chování, a zpětná vazba v reálném čase zvyšuje povědomí o správné ergonomii a podporuje preventivní opatření.

Výzvy

BOZP je zásadním aspektem každého pracoviště a je nezbytné řešit **výzvy**, které s BOZP souvisejí.

- Jednou z hlavních výzev zjištěných v případových studiích je **ochrana soukromí a údajů**. Většina systémů zahrnuje monitorování zaměstnanců, a nejen jejich pracovního prostředí, ale také dalších charakteristik, jako je zdravotní stav zaměstnanců, jejich přítomnost a blízkost k ostatním zaměstnancům. Proto je nezbytné pečlivě navrhnout systém ochrany údajů, který vyřeší dva hlavní problémy: právní rizika a obavy koncových uživatelů. Obecné nařízení o ochraně osobních údajů EU (nařízení GDPR) stanoví spolehlivá pravidla ochrany osobních údajů, a proto jsou právní důsledky v členských státech obzvláště důležité.
- Další související výzvou je **kybernetická bezpečnost**. Všechny předložené případové studie vyžadují sběr velkého množství často citlivých údajů a zařízení mohou být cílem kybernetických útoků, tudíž by tato zařízení měla být společnostmi, která nový systém zavádí, pečlivě chráněna. Obavy ohledně soukromí údajů nebo jejich zneužití se z pohledu koncových uživatelů – pracovníků – řadí k nejdůležitějším.
- Výzvy pro BOZP se mohou týkat také **potenciálních technických problémů a poruch** vedoucích ke vzniku nemonitorovaných rizik nebo narušení procesu monitorování a zpětné vazby, potenciálním falešným pozitivním a negativním výsledkům způsobujícím nesprávná upozornění a problémům s interoperabilitou a integrací dat. Tyto problémy poukazují na nutnost odpovídajícího začlenění nových systémů do stávajících rámců BOZP, aby byla zajištěna komplexní bezpečnost na pracovišti.

- Inteligentní digitální systémy s sebou přinášejí nové výzvy v oblasti řízení BOZP. Jeden často zmiňovaný problém se týká skutečnosti, že systémy pro monitorování BOZP **mohou v praxi zastřít odpovědnost za BOZP** tím, že se na ně zaměstnavatelé budou stále více spoléhat na úkor jiných – kolektivních – opatření v oblasti BOZP. Zaměstnavatelé mohou případně vypustit vhodné hodnocení rizik, nepřijmout organizační opatření nebo přistupovat k inteligentním systémům jako k náhradě za jiné povinnosti v oblasti BOZP. Zaměstnanci se také mohou stát příliš závislími na systému, potenciálně zanedbávat základní bezpečnostní postupy a lidský úsudek, nebo se mohou cítit chráněni a nést větší rizika. Z případových studií vyplynulo, že osoby zodpovědné za návrh a vývojáři (poskytovatelé) a uživatelé a zavádějící společnosti (zavádějící subjekty) věnují velkou pozornost spolupráci v zájmu pochopení potřeb na daném pracovišti, účinného začlenění nových řešení do stávajícího rámce BOZP a poskytnutí odpovídající odborné přípravy a zdrojů na pracovišti. Zásadní význam má řádná odborná příprava pracovníků a odborníci na BOZP jsou často kontaktním místem při zavádění systému, jelikož v případě jakýchkoliv obav pracovníků jsou v první linii. Aby bylo možné plně využít potenciálu těchto řešení, musí mít osoba zodpovědná za návrh znalosti potřeb a specifík podniku, které může získat pouze od osoby, která v podniku denně působí.
- Další problém pro odborníky na BOZP spočívá v nutnosti **najít rovnováhu mezi monitorováním bezpečnosti, a nikoli výkonnosti pracovníků**. Díky technologiím, které monitorují různé aspekty charakteristik pracovníků, mohou mít odborníci a společnosti působící v oblasti BOZP přístup k údajům, které výrazně přesahují rámec toho, co je nezbytné pro ochranu zdraví a bezpečnost na pracovišti. Proto musí odborníci na BOZP z právních důvodů i z důvodů zachování důvěry věnovat mnohem větší pozornost své práci, aby **zajistili, že osobní údaje pracovníků jsou v bezpečí a používají se pouze pro účely bezpečnosti**. Z dlouhodobého hlediska existuje možnost, že při provádění takovýchto úkolů nahradí odborníky na BOZP technologie podporovaná umělou inteligencí.
- Orgány inspekce práce se rovněž potýkají s problémy souvisejícími s technologiemi v oblasti BOZP. Bezprostřední výzvou je, že vytvářejí překážku vstupu pro inspektory. Inspektoři by si rovněž měli být vědomi rizika přílišné závislosti na technologii, nepřesnosti dat a manipulace s nimi. Inteligentní digitální systémy by proto měly být používány spíše jako podpora inspekce než jako její náhrada.
- V několika případových studiích byly vyjádřeny obavy zaměstnanců, což poukazuje na výhrady vůči každodennímu používání technologií v oblasti BOZP. V různých podnicích vyjadřují zaměstnanci obavy ohledně monitorování jejich produktivity a možného zneužívání údajů. Obávají se, že **budou sdílet údaje o své produktivitě a poloze se svými vedoucími, a mají obavy, že „když budou unavení, dostanou výpověď“**. Zaměstnanci se obávají, že pracovní zátěž se může zvýšit kvůli přesvědčení, že jsou lépe chráněni, například tak, že se od jednoho zaměstnance bude vyžadovat, aby zastal práci, kterou obvykle dělají dva lidé. Další obavy koncových uživatelů se týkaly pohodlí zaměstnanců, které může negativně ovlivnit jejich výkonnost. Další častou obavou zaměstnanců je ochrana údajů. Technologie může zachytit jejich okolí a může je sledovat. Zaměstnanci se obávají, že budou sdíleny jejich údaje o zdravotních problémech. Objevily se obavy ohledně možných bezpečnostních rizik spojených s rozsáhlými operacemi.
- Na základě shromážděných dat lze předestřít možné výzvy **týkající se ochrany možnosti pracovníků mít slovo při rozhodování** a obecněji jejich zapojení. *Přílišná závislost* na (velmi kvantitativních) datech získaných z inteligentních digitálních systémů, aniž by bylo nutné získat přímou zpětnou vazbu od zaměstnanců, může vést k *mylným výkladům a rozhodnutím, která nejsou optimální, a dokonce škodlivá*, a to jak z hlediska BOZP, tak z hlediska provozu podniku. Zavádění takových systémů by tedy mělo být doprovázeno postupy pro zapojení zaměstnanců nad rámec fáze zaškolení; a čím větší narušení soukromí představuje sběr údajů a možné důsledky používání systému pro provoz společnosti, tím větší by mělo být **zapojení**

zaměstnanců. Zainteresovaní zaměstnanci mohou také **zajistit, aby se odpovědnost za BOZP nepřesunula z kolektivní úrovně na individuální.**

Bylo zjištěno několik opatření, která mají řešit obavy zaměstnanců v souvislosti s technologiemi v oblasti BOZP. Tato opatření se zaměřují na to, jaké údaje jsou shromažďovány a jak jsou uchovávány. V některých případových studiích se monitorování dat vztahuje k danému zařízení, nikoli osobě, která zařízení používá, což představuje další bezpečnostní vrstvu pro anonymitu zaměstnanců. Mezi další opatření patří vybízení vedení společnosti, aby se písemně zavázalo, že technologie nebude zneužita k jiným účelům než BOZP.

Uvedené obavy pracovníků se zaměřují na **zásadní otázku důvěry** mezi pracovníky a zaměstnavateli. Mají-li se skutečně řešit obavy, měly by inteligentní digitální systémy zahrnovat řešení, která zaručí důvěru. To zahrnuje zabudování funkcí, které dávají pracovníkům možnost zjistit konkrétní kroky zaměstnavatele týkající se jejich údajů a kontrolovat zpracování údajů (včetně jeho ukončení), pokud zpracování nemá legitimní základ nebo přesahuje stanovený účel. Vzhledem k **nerovnováze moci** by měly být právní systémy rovněž připraveny chránit pracovníky, kteří tímto způsobem uplatňují svá práva.

Kromě právních předpisů mají jasnou úlohu ve způsobu zavádění a používání inteligentních digitálních systémů také **inspekce práce**. Aby však mohly inspekce práce tuto úlohu plnit, musí být vybaveny odbornými znalostmi a zdroji. V tomto smyslu musí právní předpisy a inspekce práce držet krok s rychlým rozvojem inteligentních digitálních systémů a jejich používáním na pracovišti, aby bylo zajištěno jejich začlenění do účinného systému řízení BOZP založeného na kolektivní odpovědnosti zaměstnavatele a v kontextu hierarchie kontrol.

5 Obecné závěry a úvahy

S ohledem na informace shromážděné v případových studiích bylo vyvozeno několik závěrů a doporučení.

Proaktivní a reaktivní funkce inteligentních digitálních systémů

S ohledem na široké důsledky je třeba poznamenat, že hnací silou zavádění inteligentních digitálních systémů je celkově **snaha o zvýšení bezpečnosti a ochrany zdraví na pracovištích**, což je cíl, který sám o sobě není nový, ale lze jej dosáhnout využitím nejmodernějších technologií.

Díky poskytování dat v reálném čase, prediktivním poznatkům, a dokonce vykonatelným doporučením mohou nové **monitorovací systémy významně přispět k proaktivnímu přístupu k BOZP**. Namísto pouhé reakce na incidenty mohou společnosti předvídat rizika, předcházet úrazům a chránit své zaměstnance. V případových studiích se uvádí příklad toho, jak technologie umožňují identifikaci a včasné odhalení rizik, což vede k prevenci nebo zamezení škod. Spektrum rizik, jimiž se případové studie zabývají, je široké a sahá od individuálních a kolektivních škodlivých expozic a úrovní životního prostředí přes expozici ergonomickým rizikům až po psychosociální rizika.

Vzhledem k technologickému vývoji lze získat přesné a rychlé poznatky, pokud určité parametry překračují konkrétní prahové hodnoty nebo normy. Jak ukazují některé případové studie, odhalování rizik lze dále posílit pomocí **prediktivních algoritmů, které mohou analyzovat složité nebo historické systematičnosti v datech, včetně dat velkého objemu, a předpovídat potenciální rizika a poskytovat poznatky o chování.**

Kromě toho, pokud jde o důsledky pro řízení BOZP, systémy nabízejí **provozní příležitosti pro společnosti a odborníky na BOZP**. Některé systémy například umožňují provádět interní hodnocení rizik, inspekce nebo audity na dálku, což šetří čas a zdroje, které by jinak byly nutné pro cesty do vzdálených provozoven. Vzdálené technologie rovněž mohou umožnit účast externích stran na těchto hodnoceních a inspekcích. Jiné systémy mohou zvýšit účinnost kontroly dodržování předpisů tím, že zjišťují, zda jsou používány ochranné prostředky, dodržovány postupy a zda je zařízení správně provozováno.

Rozsáhlé využívání dat podporované umělou inteligencí a strojovým učením může odborníkům na BOZP a zaměstnavatelům pomoci lépe **pochopit situaci na jejich pracovištích a usnadnit neustálé**

zlepšování, tj. umožnit přizpůsobení systémů na úrovni podniku a interních postupů za účelem dalšího zlepšení bezpečnosti na pracovišti. Spolu s větším potenciálem prezentovat informace přizpůsobené potřebám konkrétních zaměstnanců nebo skupin mohou digitální technologie posílit funkce systémů BOZP v oblasti odborné přípravy. V případových studiích nebyly přímo identifikovány systémy používané pro účely inspektorátů práce. Takové použití si však zjevně lze představit a v průběhu výzkumu byly zmapovány mnohé příklady.¹⁰

Jak dokládají případové studie, inteligentní digitální systémy v praxi často slouží více účelům v oblasti BOZP a kombinují více než jednu digitální technologii. Často se neomezují na monitorování více rizikových faktorů v rámci proaktivních funkcí systémů, ale také zahrnují funkce, které spadají do kategorie reaktivního monitorování BOZP. Tím, že systémy umožňují snadnou signalizaci a přesnou lokalizaci nouzových situací a pomáhají reagovat na tyto události, mohou minimalizovat důsledky újm, ke které na pracovišti došlo.

Nové technologické schopnosti mohou rovněž zlepšit způsob, jakým jsou úrazy vyšetřovány, hlášeny a využívány na podporu zlepšení BOZP. I když inteligentní systémy přinášejí mnoho příležitostí, představují pro BOZP také výzvy. Z analýzy provedených případových studií vyplývá, že klíčem k překonání těchto výzev je způsob, jakým jsou systémy začleněny do stávajících rámců BOZP.

Začlenění inteligentních digitálních systémů do stávajících rámců BOZP

Při zdůraznění multifunkčnosti řešení, o nichž pojednávají případové studie, je zřejmé, že v některých případech se jedná o **integrované systémy**, jejichž cílem je nabídnout komplexní řešení pro využití nového technologického pokroku a kombinací technologií uspokojují specifické potřeby odvětví, podniku nebo pracoviště. Tím, že poskytují přesné a podrobné monitorování různých parametrů, mohou výrazně zlepšit postupy v oblasti BOZP a přispět k bezpečnějšímu pracovnímu prostředí. BOZP je však proces nebo cyklus, a nikoli izolovaný zásah, a ačkoli jsou systémy schopny vykonávat mnoho funkcí, systémy, o nichž se v této studii pojednává, nedokážou (ani to není jejich cílem) poskytovat řešení „vše v jednom“. Na rámec BOZP je třeba pohlížet jako na prostředek neustálého učení, který zahrnuje řadu závislostí, procesů a postupů. Jedná se tedy o rámec, který **zahrnuje širší škálu prvků než jeden inteligentní systém monitorování**.

Při zkoumání případových studií se ukazuje, že tyto inteligentní digitální systémy jsou často **cíleně koncipovány tak, aby řešily konkrétní účely nebo monitorovaly konkrétní parametry**. Ať už se jedná o specifická odvětví, sektory nebo jednotlivé společnosti, tyto systémy jsou přizpůsobeny jedinečným požadavkům. Bohatství informací, které přinášejí, umožňuje cílené intervence a proaktivní opatření. Například systém navržený ke sledování hladiny hluku ve výrobním závodě se může výrazně lišit od systému zaměřeného na posouzení ergonomie v kancelářském prostředí. Tato přizpůsobivost může potenciálně **zajistit, aby monitorování BOZP bylo v souladu se specifickými potřebami v každém jednotlivém kontextu**.

I když systémy jsou do určité míry přenositelné (čím podobnější jsou úkoly, užití nebo odvětví, tím vyšší je přenositelnost), v případových studiích se zdůrazňuje, že zavedení na konkrétním pracovišti vyžaduje určité zamyšlení. Úzká spolupráce mezi vývojářem a zavádějícím subjektem a **jednotné chápání potřeb a priorit zaměstnanců jsou zásadní pro zaručení úspěšného zavedení řešení**. Vývojáři a uživatelé systému musí řešit potřeby na úrovni zaměstnavatele (vrcholového managementu), na úrovni odborníků na BOZP a na úrovni zaměstnanců společnosti. Ve zkoumaných případech to často probíhalo prostřednictvím opakujících se výměn názorů mezi vývojářem a společnostmi, které byly uživateli. Tyto výměny sloužily k posouzení účinnosti systému a identifikaci prostoru pro zlepšení.

Důležitost pochopení potřeb a priorit souvisí se skutečností, že data shromážděná inteligentními digitálními systémy mohou být potenciálně nepřesná, omezená nebo zkreslená, což v konečném důsledku může přinést rizika pro bezpečnost a zdraví. **Nadměrná závislost na inteligentních systémech může vést k sebeuspokojení a falešnému pocitu bezpečí**, což může být obzvláště nebezpečné ve vysoce rizikových pracovních prostředích. Proto je velmi důležité, aby se tyto systémy

¹⁰ EU-OSHA – Evropská agentura pro bezpečnost a ochranu zdraví při práci, *Inteligentní digitální systémy pro monitorování bezpečnosti a ochrany zdraví při práci: využití a související výzvy*, 2022. https://osha.europa.eu/sites/default/files/Smart-digital-monitoring-systems-uses-challenges_en.pdf

používaly jako **doplněk** tradičních bezpečnostních opatření a lidského úsudku, které tvoří prvky širšího rámce BOZP, **a nikoli jako náhrada** za ně.

Pracoviště jako prostředí bohaté na data

Zavádění digitálních technologií na pracovišti přináší četné příležitosti a výzvy. Základní změna spočívá v tom, že inteligentní digitální systémy – jako součást širších rámců BOZP – transformují pracoviště na prostředí bohaté na data, a tudíž **se primární hlediska týkají soukromí údajů pracovníků a možného zneužití těchto údajů**.

Z případových studií vyplývá, že inteligentní digitální systémy, které slouží ke zvýšení bezpečnosti a obecněji dobrých pracovních podmínek pracovníků, jsou často vnímány (a prodávány) jako nástroje, jejichž primárním uživatelem je zaměstnavatel. Pracovníci mohou být motivováni k tomu, aby se v některých fázích podíleli například na navrhování nebo zavádění systémů na pracovišti, a jsou vyškoleni k jejich používání, ale rozhodnutí o zavedení nového systému přijímá společnost/zaměstnavatel.

Díky těmto systémům získávají podniky informace, které mohou být významné pro zlepšení BOZP, ale poznatky, které získávají o pracovnících, **prohlubují asymetrii, která je nedílnou součástí pracovněprávních vztahů**. U některých typů systémů, jako jsou systémy shromažďující biometrické údaje, může tato asymetrie dosáhnout úrovně, kdy zaměstnavatelé vědí o svých pracovnících mnohem více než pracovníci sami o sobě.

Zavádění takových systémů by tedy mělo být **doprovázeno postupy pro zapojení zaměstnanců nad rámec fáze zaškolení**; a čím větší narušení soukromí představuje sběr údajů a možné důsledky používání systému pro provoz společnosti, tím vyšší by mělo být zapojení pracovníků. Konkrétní opatření a postupy budou vždy záviset na důvodech zavedení systému, ale musí se rovněž zabývat tím, jaké údaje jsou shromažďovány a jak jsou uchovávány a zpracovávány. Ve zkoumaných případech se zdůrazňují dva přístupy k těmto otázkám: **a) ochrana soukromí již od návrhu**, což zahrnuje opatření, jako je anonymizace údajů, minimalizace údajů, dodržování obecného nařízení o ochraně osobních údajů a bezpečné uchovávání údajů, a **b) ochrana soukromí na základě rozhodnutí**, která se zaměřuje na omezení přístupu k údajům na konkrétní pracovní pozice a uživatele (např. odborníky na BOZP).

Při zběžném pohledu mohou být obavy týkající se soukromí údajů nebo zneužití, které zaměstnanci uvedli, *vnímány jako odpor* vůči novým technologiím. Toto vnímání svědčí o možném implicitním přijetí nevyhnutelnosti zavedení těchto systémů zaměstnavateli. Obavy týkající se umožnění přístupu zaměstnavatelů ke stále většímu počtu sfér života zaměstnanců, včetně duševního zdraví, jsou však závažné a jsou příčinou toho, proč se někteří zaměstnanci vyslovili proti používání některých technologií. To poukazuje na to, že **při zavádění digitálních inteligentních systémů na pracovišti je třeba brát v úvahu ochranu údajů a případně vypracovat pokyny či předpisy, které ochrání práva zaměstnanců**. Inteligentní digitální systémy by měly zahrnovat funkce, které dávají zaměstnancům možnost zjistit konkrétní kroky zaměstnavatele týkající se jejich údajů a kontrolovat zpracování údajů (včetně jeho ukončení), pokud zpracování nemá legitimní základ nebo přesahuje stanovený účel. Vzhledem k nerovnováze sil, která je nedílnou součástí vztahu zaměstnanec-zaměstnavatel, by měly být právní systémy rovněž připraveny chránit pracovníky, kteří tímto způsobem uplatňují svá práva. Kromě právních předpisů mají jasnou úlohu ve způsobu zavádění a používání nových systémů také **inspekce práce**.

6 Hlavní poznatky pro rozvoj a zavádění inteligentních digitálních systémů v oblasti BOZP

Na základě případových studií lze formulovat řadu průřezových poznatků a úvah pro vývoj a zavádění inteligentních digitálních systémů. Do jisté míry se překrývají, což jen podtrhuje, že některé problémy, jako je bezpečnost a ochrana osobních údajů a spolupráce, by měli zvážit jak tvůrci systému (poskytovatelé), tak i osoby odpovědné za zavádění (zavádějící subjekty).

Rámeček 1: Nad čím by se měli zamyslet vývojáři inteligentních digitálních systémů

Návrh a vývoj systému by měl v příslušných případech zajistit následující funkce:

INTEGRACE A PŘÍZPŮSOBNOST PODLE POTŘEB

- **Integrace do stávajících systémů organizací s cílem optimalizovat procesy BOZP** a vytvoření uceleného pohledu na bezpečnost a ochranu zdraví na všech pracovištích, předcházení problémům s migrací a předvídání (budoucí) potřeby v souvislosti s přizpůsobitelností.
- **Přizpůsobení** tak, aby vyhovovaly konkrétním organizačním a individuálním potřebám.
- **Individualizace** díky zabudování **zásad rozmanitosti a začleňování**.
- **Návrh ze své podstaty má zabránit negativním důsledkům** používání inteligentních monitorovacích systémů pro měření výkonnosti.
- **Podpora proaktivního řízení bezpečnosti** s cílem klást důraz na zmírňování rizik před výskytem incidentů, což se ukazuje jako jednoznačně výhodnější oproti reaktivním technologiím.

ZABEZPEČENÍ ÚDAJŮ A SOUKROMÍ

- **Soulad** s platnými příslušnými právními předpisy (evropskými i vnitrostátními) v otázkách, jako je ochrana osobních údajů, ustanovení (o umělé inteligenci) atd.
- **Podpora návrhu zaměřeného na ochranu soukromí**, který se zabývá obavami v souvislosti s ochranou soukromí zaměstnanců a zmírňuje je a do něhož je začleněna ochrana soukromí již od návrhu, je-li to proveditelné nebo jedná-li se o upřednostňovanou možnost.
- **Minimalizace a/nebo anonymizace shromážděných údajů**, zabránění shromažďování údajů, které nejsou relevantní pro BOZP, a zpřístupnění určitých prvků, jako jsou údaje o zeměpisné poloze, pouze za určitých okolností, například v případě vydání upozornění.
- **Transparentnost díky jasnému informování uživatelů** o aspektech ochrany údajů a řízení systémů s cílem zachovat a vybudovat důvěru mezi zaměstnanci.
- **Zajištění spolehlivých opatření pro bezpečnost údajů** v rámci systému s cílem řešit potenciální kybernetické útoky a zajistit důvěrnou povahu údajů uživatelů.

SPOLEHLIVOST A UŽIVATELSKÁ PŘÍVĚTIVOST

- **Zajištění pohodlí uživatele** při navrhování nositelných zařízení a přístrojů.
- **Zaměření se na bezpečná rozhraní** pomocí ergonomického a intuitivního designu, v jehož středu zájmu stojí uživatel, pokud jde o rozhraní, s cílem minimalizovat fyzická a provozní rizika.
- **Zvýšení přesnosti** prostřednictvím průběžné empirické validace a zpřesnění algoritmů a zdrojů údajů, čímž se zajistí spolehlivé výsledky pro potřeby klientů.
- **Uvedení do souladu s příslušnými normami** pro účinný provoz v **náročných prostředích a odlehklých oblastech**.
- Dodržování transparentních a striktních postupů s cílem zajistit **jasnost, pokud jde o to, jak se od údajů dospělo k interpretaci, a zabránit možným zkreslením, a to i těm nezáměrným**.

KOMUNIKACE A SPOLUPRÁCE

- **Jasně informování potenciálních klientů o omezení systémů**, aby se zabránilo nedorozuměním ohledně jejich používání.
- **Zapojení zástupců klienta**, zejména uživatelů a pracovníků, do fáze vývoje.
- **Transparentnost zaváděním opatření**, která klientům poskytují **jasný vhled** do fungování

systémů a informují o **výchozích algoritmech**, což podpoří důvěru a porozumění.

- **Vytvoření rámce pro spolupráci krok za krokem** se zavádějícími subjekty s důrazem na účinné **řízení změn** a komunikaci.
- **Nabídka průběžné podpory** pro zavádějící subjekty během celé fáze zavádění, jako jsou zkušební období, testovací fáze, výukové programy, workshopy, uživatelské příručky, návštěvy na místě atd.

Rámeček 2: Nad čím by se měli zamyslet uživatelé / zavádějící subjekty (zaměstnavatelé) inteligentních digitálních systémů

Zavádění systému by mělo ve vhodných případech zahrnovat následující prvky:

ZABEZPEČENÍ ÚDAJŮ A SOUKROMÍ

Na co je třeba dbát při zavádění systémů:

- **Uvedení do souladu** s platnými evropskými a vnitrostátními právními předpisy o ochraně osobních údajů a relevantních technologiích (AI).
- **Minimalizace a/nebo anonymizace shromážděných údajů**, zabránění shromažďování údajů, které nejsou relevantní pro BOZP, a zpřístupnění určitých prvků, jako jsou údaje o zeměpisné poloze, pouze za určitých okolností, například v případě vydání upozornění.
- **Zajištění spolehlivých opatření pro bezpečnost údajů** v rámci systému s cílem řešit potenciální kybernetické útoky a zajistit důvěrnou povahu údajů uživatelů.
- **Zapojení pracovníků nebo jejich zástupců za účelem řešení obav** týkajících se shromažďování osobních údajů, poskytování komplexních informací a stanovení jasných zásad týkajících se využívání údajů a monitorování pracovníků, zajištění transparentnosti a souhlasu.
- **Stanovení jasných protokolů a postupů** pro řešení veškerých obav nebo problémů, na které pracovníci upozorní v souvislosti se soukromím, zabezpečením údajů nebo etickými hledisky.

ÚČEL POUŽÍVÁNÍ SYSTÉMU A PROAKTIVNÍ KULTURA BEZPEČNOSTI

- **Ochrana práv zaměstnanců** a jasné informování uživatelů o aspektech ochrany osobních údajů a správy systémů, přijetí transparentního přístupu s cílem vybudovat důvěru v řadách zaměstnanců.
- **Podpora postupů a zásad**, v nichž se definují účely a působnost používání systému a objasňuje se, kdo **je vlastníkem shromážděných údajů**, a srozumitelné informování o těchto postupech a zásadách.
- **Oddělení systému BOZP od ostatních systémů správy informací**, například těch, které se týkají měření výkonnosti pracovníků, aby byla zajištěna transparentnost a překonán odpor zaměstnanců.
- **Poskytování komplexní odborné přípravy** zaměstnancům ohledně správného používání a výkladu systému a zdůrazňování jeho úlohy jakožto podpůrného nástroje, nikoliv dohledového mechanismu.
- **Na základě poznatků získaných z dat přijetí kroků s cílem podpořit proaktivní kulturu bezpečnosti** na pracovišti a účinná nabídka podpory a poradenství pro ohrožené zaměstnance.
- **Podpora proaktivního řízení bezpečnosti** s cílem klást důraz na zmírňování rizik před výskytem incidentů, což se ukazuje jako jednoznačně výhodnější oproti reaktivním technologiím.

- **Podpora vyvážené ostražitosti** – podporuje rovnováhu mezi spoléháním se na technologii a lidskou ostražitostí prostřednictvím programů odborné přípravy a osvětových programů.

INTEGRACE SE STÁVAJÍCÍMI RÁMCI A TECHNICKOU INFRASTRUKTUROU V OBLASTI BOZP

- **Uznání, že hlavní odpovědnost** za zajištění bezpečnosti na pracovišti nesou **zaměstnavatelé** a že ji nelze nahradit ukazateli v systému.
- **Zdůraznění toho, jak nový systém podporuje individuální dobré pracovní podmínky**, povzbuzování pracovníků k tomu, aby přijali preventivní opatření pro vlastní bezpečnost, a zároveň připomenutí, že **zaměstnavatel má i nadále celkovou odpovědnost za BOZP**.
- Zavedení nových inteligentních digitálních systémů jako **nedílné součásti komplexního rámce BOZP**, a nikoli jako jeho náhrady.
- **Prozkoumání možností, jak zlepšit integraci (a interoperabilitu) systému** s cílem optimalizovat procesy BOZP a vytvořit **ucelený pohled na bezpečnost a ochranu zdraví na všech pracovištích**, předcházet problémům s migrací a předvídat (budoucí) potřeby v souvislosti se škálovatelností.
- Zejména při operacích, při kterých může dojít k ohrožení života. Zavedení jasných protokolů a postupů **pro řešení veškerých obav nebo problémů, na které pracovníci upozorní v souvislosti se soukromím, zabezpečením údajů a etickými hledisky**
- **Provádění pravidelných hodnocení a posuzování** účinnosti systému a jeho dopadu na dobré pracovní podmínky pracovníků a podle potřeby provádění úprav, aby bylo zajištěno jeho bezpečné a odpovědné zavádění.
- **Vyčlenění dostatečných zdrojů** pro řádné zavedení a pravidelnou údržbu systému a přijetí preventivních opatření proti případným poruchám systému.

SPOLUPRÁCE S VÝVOJÁŘI SYSTÉMU

- **Zajištění transparentní komunikace s vývojáři systémů** s cílem získat jasné informace o omezeních a vzhled do fungování systémů a výchozích algoritmů, což podporuje důvěru a porozumění.
- **Zapojování zástupců zaměstnanců během zavádění systému** s cílem zajistit individualizaci a přizpůsobení jejich potřebám, jakož i posílit důvěru a transparentnost.
- **Vytvoření rámce pro spolupráci krok za krokem** s vývojářem s důrazem na účinné řízení změn a komunikaci.
- **Nabídka průběžné podpory od vývojáře** během celé fáze zavádění, jako jsou zkušební období, testovací fáze, výukové programy, workshopy, uživatelské příručky a návštěvy na místě.

**Evropská agentura pro bezpečnost
a ochranu zdraví při práci (EU-OSHA)**

přispívá k cíli učinit z Evropy bezpečnější, zdravější a produktivnější místo pro práci. Agentura provádí výzkum, vývoj a distribuci spolehlivých, vyvážených a nestranných informací v oblasti BOZP a pořádá celoevropské osvětové kampaně. Agentura, kterou Evropská unie zřídila v roce 1994 a která sídlí ve španělském Bilbao, umožňuje spolupráci zástupců Evropské komise, vlád členských států, organizací zaměstnavatelů a zaměstnanců i předních odborníků ze všech členských států Evropské unie i dalších zemí.

**Evropská agentura
pro bezpečnost a ochranu zdraví při
práci**

Santiago de Compostela 12
48003 – Bilbao, Španělsko
E-mail: information@osha.europa.eu
<http://osha.europa.eu>