Soukromí má cenu

pět stránek o falešných argumentech a světýlku na konci tunelu

Oldřich Kužílek
poradce pro ochranu soukromí a otevřenost veřejné správ, člen Rady vlády pro lidská práva

Obsah:

1. 3 alibi

Při ochraně osobních údajů (a šířeji soukromí) jsem vypozoroval **tři druhy obtíží,** se kterými se dnes setkáváme. Tyto obtíže jsou třemi druhy **rezignace** na obranu lidské svobody. Jsou to vlastně tři různá **alibi**, která uvádějí nejen **pachatelé** takového či onakého zásahu do ochrany soukromí, ale bohužel i ti, kteří jsou **povinni čelit** rozpínavosti státu a techniky, pokud omezují lidskou svobodu.

Okno bez záclony

Využívání osobních údajů a informací o soukromí prý vlastně nevadí, protože když člověk nic špatného nedělá, nevadí mu, že je na něj vidět. Typickým projevem této rezignace bylo prohlášení policejního presidenta Koláře v roce 2002, že mu nevadí, kdyby byl odposlouchávaný, protože je nic špatného nedělá.

Goliáš

Druhým alibi je, že jakýkoli **boj** proti rozšíření moderních technologií **je marný.** Soukromý sektor i stát bude tato zařízení, sledující doslova kdeco, využívat stále více, protože jde jak o byznys, tak o efektivitu a zjednodušení mnoha činností. Typickým projevem je nedávno zavedený systém centrální evidence výdeje léků v lékárnách, který vznikl hlavně proto, aby bylo možno rozšířit okruh léků vydávaných bez lékařského předpisu. Pak je ale nutné odběratele těch, které mohou být zneužity k výrobě drog, evidovat, zda si jich neberou moc. Zdánlivá efektivita centrálního evidování a kontrolování čehokoliv zde zastínila otázku, zda je takové opatření přiměřené exkluzivnímu účelu.

Sezame, otevři se

Třetím alibi pro rezignaci zní: „osobní údaje jsou **dostatečně ochráněny** přidělením **přístupových práv, hesel a kontroly přístupů konkrétních uživatelů."** Tento argument je omílaný ve všech důvodových zprávách návrhů zákonů, které upravují různá zpracování osobních údajů. Typickým příkladem byla bitva, kterou museli svést ochránci osobních údajů (jak ze sdružení eStat, tak z Úřadu pro ochranu osobních údajů) s ministerstvem vnitra o to, aby systém základních registrů veřejné správy byl od základu zabezpečený pomocí další, jiné a ne-softwarové vrstvy organizačního opatření, na principu oddělených identifikátorů.

Pokusím se tato tři alibi vyvrátit.

Okno bez záclony versus síla paralelní reality

Shromažďované údaje vytvářejí **paralelní, informační** a tedy zdánlivě imaginární realitu, **částečně kopírující** prvotní, tradičně prožívanou realitu. Jejich vztah ale není imaginární. Paralelní realita umí silně zasáhnout do prvotní reality. V politickém prostředí se to již několikrát s citelnými dopady stalo. Příkladem je kauza hotelu **Savoy**, kdy paralelní realita (záznamy pohybu konkrétních osob) ovlivnila volbu presidenta republiky. Jiný příklad: nezjištěný policista vyrobil falešné výpisy hovorů osoby vyšetřované pro daňové úniky s úmyslem diskreditovat na jejich základě politiky, s nimiž údajně telefonoval. Pod přístupovými kódy jiného policisty došlo na počítači k obměně a výtisku výpisů, do kterých byly přidány jiné hovory.
Pamatujeme případ muže, který několik let nemohl normálně žít, protože **došlo k záměně jeho rodného čísla**. Podobné jsou některé **zákroky exekutorů**, kteří vycházejí z nedokonalých veřejných registrů, tedy z nedokonalé paralelní reality.
Vzhledem k existenci rozsáhlých databází pohybu osob v Praze (například úsekové měření rychlosti a průjezdu na červenou, zaznamenávající přítomnost konkrétní registrační značky vozidla včetně fotografie řidiče a spolujezdce několik let dozadu na asi 20 frekventovaných místech) si lze snadno představit, že **údaj z takové databáze může významně ovlivnit život člověka**, který se dostane do hledáčku policie proto, že v databázi bude k jeho přítomnosti uveden určitý časový údaj. Tak se **ze slušného občana může stát podezřelý z vraždy**. Přitom změna časového údaje o několik sekund může být klíčová.

Závěr: Paralelní realita tedy má zatraceně silný vliv na naše životy.

Goliáš versus David

Nové technologie již v dějinách vícekrát přinesly významná rizika. Obvykle se daří najít **mechanismus, jak dostat džina zpět do láhve.** Základem je vždy **etický postoj** – pochopení, co je slušné a co je neslušné. Tento postoj pak bývá doprovozen právem, zákony, které určité chování zakáží. V průmyslové revoluci zjistilo mnoho konstruktérů a podnikatelů, že zdánlivě **nejlevnější a nejefektivnější způsob**, jak realizovat určitou technologii, je vyhodit nebo **vylít její zplodiny do přírody**. Bylo to zadarmo. Postupně se vyvinulo vědomí, že je to neslušné, že provozovatel ostatním krade cennou hodnotu – čisté životní prostředí. Dnes je to zakázané. **Morálka a právo tak přinutily Technologie uzavřít se do sebe** tak, aby nebyly schopné škodit do okolí. Toleruje se tedy například nakládání s jaderným materiálem nebo toxickými látkami, ale jen za velmi přísných a drahých opatření, která zajišťují intaktnost vůči okolí. Chráněná hodnota – čisté prostředí – tak dostala cenu, danou buď dražší technologií, výší sankce, anebo placenými limity. Nejefektivnější jsou tak provozy, které se škodlivým postupům úplně vyhnou.
Podobný je obecný zákaz, aby na veřejnosti někdo **mával ostře nabitou zbraní** nebo jel **autem s nefunkčními brzdami**.
Stejně je třeba pochopit, že nejen přírodní, ale i **sociální prostředí** se musí uchovávat **v určitém smyslu čisté.** Vytváření různých **databází paralelní reality** je třeba vnímat jako **znečištění**, **riziko,** a tedy jako **neslušné či alespoň vysoce rizikové chování.** Morální postoj je třeba doprovodit právem, rozumnou regulací a jejím efektivním prosazováním, aby se do technologie promítly skutečné náklady, neboli aby se **do její ceny promítla cena „ukradené svobody“.** Provozovatel raději najde jiné méně nebezpečné řešení. Příklad: Díky drobné

regulaci (dočasný zákaz měření rychlosti obecní policií) nyní obce raději kupují příjezdové semafory, kde se spustí červená, pokud auto přijíždí rychleji než smí. Tím se stejného účelu (bezpečnosti) dosáhne bez měření rychlosti se skenováním značek aut a ukládáním údajů všech slušných řidičů do databáze. Pokud nějaké město pláče, že vydalo miliony na systém sledování dopravy, který by byl po regulaci nanic, představme si totéž v rovině chemické továrny, která lká, že nebude-li vypouštět toluen do potoka, znehodnotí se milionová investice.

Závěr: Zdánlivá převaha technologií není nic nového, mnohokrát se podařilo džina dostat zpět do láhve.

Sezam versus dveře

Lidská svoboda, zejména soukromí, pohybu a získávání informací, se po tisíciletí **opírala** – aniž si to dostatečně uvědomujeme – **o nepřehlednost světa,** o možnost skrýt se v něm, a o krátkost a pomíjivost lidské paměti. Hercule **Poirot**, pokud chtěl zjistit, kdo byl u místa činu, si musel popovídat s trafikantem na rohu, s prodavačkou, a ještě najít útržek oděvu na hřebíku v plotě. Šlo mu o **informaci**, tedy o **efemérní realitu**, ale musel projít mnoha **fyzickými** dveřmi, potkat spoustu skutečných lidí a osobně jim vysvětlit, o co mu jde. Musel zaplatit taxíky, jízdenky, občas i neochotného trafikanta. Tisíce situačních bariér chránilo naši svobodu. Dnes by stačilo pustit si záběry pouliční kamery.
Donedávna policejní **vyšetřovatel musel pro mnoho údajů osobně zajít**, na obecní úřad, na berňák, do nemocnice, na pracoviště podezřelého. Všude se musel ohlásit na vrátnici, hovořit s úředníky, prokázat se průkazem. Každý ho viděl, zapamatoval si ho. Trvalo mu to mnoho hodin nebo dní.
Dnes se k velké a z hlediska efektivity pochopitelné radosti policie otevírá možnost, že si toto **vše zjistí od svého počítače**, pouhým odesláním identifikace oprávněné osoby. Celá operace může trvat několik vteřin. Její zneužitelnost je závratná.
Jakou **náhradu** namísto spleti historicky vytvořených situačních barier, které chránily naši svobodu, poskytují informační technologie? Obvykle pouze cosi, co je stejně efemérní, jako celá sféra paralelní informační reality. Různá **přístupová práva, hesla, kódování, logování, evidence přístupů**. Celá paralelní realita je chráněna **barierou ze stejného materiálu, z něhož je sama**. To, co je chráněno, i to, čím je to chráněno, je stejné povahy. Když už se tedy podaří ochranu prolomit, jedním rázem je vymalováno.
Hlavní rys této paralelní reality včetně barier, kterými se zabezpečuje proti zneužití, je **rychlost všech operací**, prakticky tedy neexistence času, a **tekutost, fluidnost informací, které lze bleskově změnit, přelít jinam, zkopírovat**.

Závěr: Zabezpečit údaje o soukromí měkkými prostředky nestačí.

2. nová definice rizika

Z výše uvedeného plynou dva důležité závěry:
1) Z hlediska hodnocení rizik je třeba brát samotnou **možnost ohrožení za již existující ohrožení.** Mezi stavem potenciálního ohrožení a realizací hrozby, například změnou či zkopírováním dat, totiž neleží žádný časový ani technologický odstup, který by obvykle mohl vést ke spuštění další ochranné reakce.
2) Pro omezení a ochranu paralelní reality před zneužitím je nutno **zavádět** nejen opatření ze stejné reality, ale kombinovat je s **opatřeními z jiné, zejména fyzické reality.** Měly by se vyžadovat **situační, organizační a další bariery**.

Příkladem je **dělené skladování dat.** Jako je v jaderné technologii nepřijatelné dát k sobě dvě nadkritická množství plutonia, protože by se spustila štěpná reakce, mohlo by být v oblasti paralelní reality vyžadovanou slušností a nařízeným technologickým postupem ukládat data vždy rozděleně tak, aby ani jedna část nedávala smysl a tedy při odcizení nezpůsobila škody. Sloučit rozdělné části tak, aby dávaly smysl, by bylo možné jen za přítomnosti jiné osoby, například vyšetřovatele, nejlépe s použitím fyzického klíče. V ochraně před nebezpečnými látkami jsou srovnatelné postupy běžné.

3. zpracování údajů bez výběru

Důležitou povinností, jak se situačně a organizačně vyhnout rizikům s vytvářením databází osobních údajů, je hned na počátku technického řetězce **omezit zpracování údajů bez výběru**: K dosahování některých jinak výhodných účelů se často nejprve monitoruje (zpracovává) široký okruh údajů o osobách, komunikaci nebo činnosti v dané situaci, a teprve následně se vyhodnocují příznaky, které teprve takové zpracování pro jednotlivé případy ospravedlňují a právně legitimizují.
Například při sledování dopravy by mělo nejprve být identifikováno porušení pravidel pomocí jiné, osobní údaje nevytvářející technologie (například laserový měřič rychlosti či indukční smyčka ve vozovce), a teprve následně by mohl být zaznamenán konkrétní přestupce (digitalizace registrační značky, fotografie řidiče). Tak vynucuje dodržování rychlosti například Prostějov. Stejné pravidlo se musí uplatnit i při kontrole mýtného.

4. strategie pro obnovení rovnováhy

Svrchovanost státu a ochrana jedince

Pokud jsme **vyvrátili tři nejčastější alibi,** proč vzdát boj za svobodu soukromí, pohybu a informací, je třeba vyjasnit si **strategii**, která by měla vést k onomu **zahnání džina do láhve**. Zde – myslím – je třeba zásadní změna paradigmatu. Musí se týkat jak **role státu v boji se zlem**, případně, jak se moderně říká, v prosazování pořádku, tak také samotného **pojetí soukromí a osobních údajů** jako cenného zboží.

Totalita

Totalitou se míní situace, kdy se nějaká moc pokouší **ovládnout totálně všechny složky života** společnosti. V tom smyslu je pravým opakem svobody, která je závislá na nepřehlednosti světa, možnosti být neviditelný, anonymní, skrytý, žít svůj osud bez zasahování. Soukromí je možnost být sám, je tedy pravým opakem totality.
.
Dnešní technologie teoreticky umožňují v určitých oblastech již téměř **totální monitorování** života. Dnes je skutečně technicky realizovatelné nastřelit všem lidem sledovací čip a monitorovat jejich polohu v každém okamžiku. Takové opatření by rázem zrušilo problém zločinu nebo přinejmenším jeho odhalování. Ekonomicky by šlo o velmi efektivní opatření, úspory by převýšily náklady velmi rychle.

Otevírá se tak zásadní a klíčová otázka, jaké může být pojetí **role státu** resp. bezpečnostních, ale i dalších správních složek veřejné moci **při boji se zlem** ve vztahu ke společnosti.

Policie není oddělena od společnosti, je její součástí, nestojí mimo ní nebo nad ní. Není archandělem Gabrielem, který s plamenným mečem sestupuje s nebe na zem a odděluje zlo od dobra. Proto je zcela principiálně **nepřijatelný pohled, že občané, společnost, jejich životy, jsou jakýmsi materiálem,** který je předhozený bezpečnostním složkám k výkonu jejich úkolů. Stát a jeho bezpečnostní orgány se musejí smířit s tím, že **pracují a budou pracovat v nepřehledném a často neprůhledném světě**, i když existují technologie, které by jim svět zpřehlednily a zprůhlednily. Pokud nám Policie argumentuje, kolik ukradených aut či prchajících zločinců vypátrala pomocí kamer, porovnejme to opět s argumentací továrny zamořující přírodu, kolik lidských životů zachránily léky, které vyrábí.
Představme si bezpečnostní složky jako **součást imunitního systému společnosti.** Obranné leukocyty smějí cokoli konat v zásadě jen **na základě skutečného napadení cizorodou látkou.** Stejně tak policie smí konat jen **na základě existujících faktů** či alespoň doložitelného podezření, že v konkrétním případě se děje něco nekalého, tedy nejprve identifikovat atak zla. **Opačný přístup,** tedy pokus technicky **uchopit totálně celou realitu**, a **následně v naskenovaném materiálu vyhledávat příznaky odchylek a porušení pravidel**, znamená, že **všichni jsou nejdříve podezřelí, aby se až následně stali nevinnými.** Pokud imunitní systém anebo policie začne monitorovat více, nebo dokonce všechno, je důsledkem alergie, rakovina, anebo ztráta imunity.

Je proto třeba **mít nástroj**, jak tuto snahu po totálním uchopení reality korigovat do míry, vždy pouze přiměřeně odpovídající na skutečnou výzvu. Jedním nástrojem je cena.

5. cíl: „cena“ soukromí

Musíme **nově začít chápat ono zboží, o které tu jde – osobní údaje**. Toto zboží má dosud prakticky **nulovou hodnotu.** Zdánlivě se totiž samo od sebe povaluje všude, po ulicích, na internetu, v databázích, k nimž je třeba pouze mít „oprávněný přístup“. **Je třeba „zdražit“ tuto dosud zlodějsky lacinou komoditu.** Domnívám se, že klíčem k tomu bude skutečnost, že osobní údaje jsou do značné míry **součástí osoby**, které se týkají. Tak jako fyzická osoba, ve smyslu fyzického těla, přesahuje do svého soukromí, do majetku od košile až po dům, tak přesahuje do informační sféry svými údaji. Tyto údaje je třeba vnímat jako součást osoby, informační auru, ba dokonce jako její vlastnictví, byť ne v klasickém, fyzickém smyslu. Nicméně je třeba **uznat právo osoby dozvědět se o každém doteku**, o nakládání s tímto svým vlastnictvím, s touto součástí své osoby. Povinnost každého zpracovatele informovat vlastníka tohoto zboží o tom, co s ním dělá, by byl systémový nástroj, který by tomuto zboží aspoň zčásti dal cenu. Navíc by zajistil informační integritu osoby, která by měla možnost vědět, co se s ní v informační sféře děje.
Takové řešení by **vycházelo z etického principu ochrany individuality**, který je euroatlantické civilizaci vlastní. Kdysi se vyvinuly pozemkové a majetkové knihy, které zajistily, že část mé osobní sféry, můj majetek, nezabere či neukradne první okolojdoucí loupežník, pokud nejsem v dohledu. Podobně bych se měl dozvědět, že se určitý úředník na druhé straně republiky podíval na moje údaje v centrálním registru.
Pokud někdo myslí, že je to **sci-fi,** měl by vědět, že tento princip se již stal součástí zákona o základních registrech, a technicky a právně nic nebrání tomu, dotáhnout ho z jednoročního souhrnného informování dotčené osoby k on-line informování v reálném čase. V některých zemích je takový on-line přístup občana k používání svých údajů ve státní správě již zavedený.