NA INTERNETU VÁS POLITICI A STÁTNÍ REŽIM MONITORUJÍ A ŠMÍRUJÍ NONSTOP I V REÁLNÉM ČASE! NA KAŽDÉHO Z VÁS VEDOU SLOŽKU. Proto nikdy nepište pod svým jménem, zásadně anonymně přes VPN. Účty vždy vytvářet bez svých osobních údajů a kontaktů!

- CZ24 News | 23. června 2022

ČESKO: Šmíruje nás kdekdo, děje se to stále častěji stále více lidem. Otázka je s pomocí jakých nástrojů nás šmírují a co proti tomu můžeme dělat.

1. **Podívat se na zástupce firem které dodávají v ČR šmírovací technologie**
2. **Popsat technologie a postupy využívané při ovlivňování veřejného mínění na jedné straně a při šmírování nás jako jednotlivců na straně druhé**
3. **Naznačit kam se posouváme ve využívání AI a vytěžování videozáznamů na příkladech z české praxe**

Technologie šmírování Čechů

Několik českých IT firem dodává státu a vybraným politikům IT řešení na šmírování občanů. Dodávají software i větším komerčním subjektům, které na to mají a pojaly nutkání monitorovat komunikaci s klienty a prohrabovat se v historii toho co kdy kdo řekl nebo napsal.

Proč se tím vůbec zabývat? Pokud pochopíme jaké zbraně má protivník a jak fungují, můžeme vymyslet vhodnou obranu nebo postupy na snížení rizik a to s ohledem na svůj životní styl. Každý jsme jiný, takže nelze doporučovat plošně.

Motivace státu je jasná. V ČR je k dnešku evidováno 656 tisíc státních zaměstnanců, kromě lékařů, hasičů a některých učitelů a ještě méně vojáků, neposkytují žádné užitečné výstupy (dobrovolně koupitelné služby nebo výrobky a zboží). Tohle udržet u moci se nedá jen s pomocí běžných odposlechů nebo šmírování ala Brettschneider ze Švejka. Dfens na těchto stránkách často píše, že nemáme s orgány státní moci, policajty, úředními pijavicemi a spol. mluvit, nad rámec nejnutnějšího, protože co řejneme, může být a bude použito proti nám. Tahle rada mě již dvakrát zachránila. Je to triviální ale účinné. Bohužel by to chtělo menší update, nic totiž říkat nemusíte, oni si najdou co píšete nebo říkáte a umí to strojově vyhodnocovat. A to i mnoho let zpětně.

Přesto se cítíte bezpečně? Zde jsou příklady důvodů, proč byste mohli změnit názor:

1. Jedna z dále představených IT firem svou technologií **pomohla Andreji Babišovi vyhrát historicky první volby** a je pravděpodobné, že se tento scénář cca zopakuje. Pokud imigranta nepovažujete za hrozbu nebo ho adorujete, třeba vás osloví druhý důvod.

2. **EU rozjíždí kombajn na plošný monitoring soukromé komunikace**, včetně částečně end-to-end šifrované, jako je WhatsApp a další. Pod záminkou boje proti dětské pornografii a zneužívání dětí, kterýžto důvod nelze sestřelit. Transpozice do legislativy ČR a definice podmínek pro využití vhodných IT řešení se ujali Piráti, což jsou fanatici (jak dokázali čerstvě i na zákazu spalovacích motorů). A proč o tom přemýšlet právě nyní? Protože je zde třetí zjevný důvod.
3. **Trh s IT šmírovacími nástroji bobtná pod vlivem grantů, dotací a rostoucích zakázek od státu a velkých korporací**. Do hry se zapojují stále vyspělejší nástroje jako AI (artificial intelligence – umělá inteligence). ČR najíždí na další level což je vyhodnocování video streamů v pilně budované sítě kamer na veřejných místech.

V ČR se je řada firem, zaměřujících se na big-datovou analytiku, sledují a vyhodnocují chování a preference skupin lidí, segmentů, davu ale i jednotlivců. Datově analytické (šmírovací) technologie, musí být ale pro získávání dat šité na míru České republice, díky specifikům češtiny. IT nástroje pro analýzu češtiny nejsou tak rozvinuté jako např. pro angličtinu a pokud jsou, stát je zatím neumí levně integrovat do svých IT systémů. Použitelné nástroje dodává na špičkové úrovni jen pár firem.

Sílu rychlé, precizní analýzy dat odhalili nacisti, kteří využívali přes Švýcarsko dodané počítače IBM (viz např. text Der Programierte Massenmord na německém Spiegelu).

O některých šmíráckých firmách jsou již na Dfensu opakovaně zmínky. Platíte si ale i neviditelné firmy, které na vašich datech usilovně pracují právě teď a o jejichž existenci nemáte tušení.

Semantic Visions

Semantic Visions je veřejně známý dodavatel průzkumů nálad ve společnosti. Vytěžují tisk, weby, diskuse sociální sítě a analyzují tam nalezené texty. Firmu reprezentuje „datový vědec“ František Vrábel. Opravdový data scientist není, ale to je jedno, stejně jako je jedno zda firmu skutečně vlastní on nebo někomu dělá bílého koně. Vystupuje za Semantic Visions a prezentuje její analýzy v médiích, tématicky zjevně na zakázku. Vytváří si pozici nestranné autority, sledující z povzdálí nálady ve společnosti. V první volbě Andreje Babiše poskytovali Semantic Visions volebnímu týmu monitoring tisku. V průběhu kampaně měřili, jak tisk reaguje na Babišovy názory a jak často a v jakých souvislostech se o něm píše. Na základě těchto zjištění volební tým optimalizoval výběr témat s největším dopadem, která Babiš poté československy drmolil na kameru. Dělali to dobře a dělali to rychle s plným nasazením a i díky Semantic Visions jsme dnes tam, kde jsme.

Semantic Visions vytěžuje již přes 10 let weby po celém světě a prodává jejich extrakty, **S**tahují terabyty dat z celého světa, od Číny po Antarktidu. Prakticky fungují jako kombajn, který sklízí web a kterým pouští dotazy a v rámci sémantické analýzy textu zjišťují frekvenci výskytu témat. Nemá smysl zde rozebírat zda toto lze vůbec legálně dělat bez souhlasu vlastníků dat. Prostě to dělají. Semantic Visions dlouhodobě vytváří zdání komerční firmy, pracující pro světové firmy. Může však jít jen o projekty tzv. ověření technického konceptu nebo projekty malého rozsahu, které jsou firmy ochotny nakoupit, ale nedostanou se do fáze zralého produkčního řešení. Na slušnou obživu, obvyklou kolem úspěšných big datových startupů, toto nestačí. Něco málo do komerční sféry i do zahraničí prodali, ale těžiště lze hledat v české kotlině, kde se profilují jako nezávislý analytický zdroj. To jsme viděli ve vystupování v průběhu COVIDu a názory pana Vrábela lze očekávat i na válku na Ukrajině a jistě se projeví v oblasti volebních preferencí Babiše.

Nová kampaň budoucího českého prezidenta ČR, Slováka Babiše, je postavena jinak, IT nástroje pro průběžnou analýzu dopadu kampaně jedou již na plné obrátky. Model je jednoduchý: lidé, se kterými se fragmentovaná voličská základna dokáže ztotožnit, oslovují za Babiše a prohlašují, že za Babiše bylo líp. Spoléhají na hospodářský propad který nastává se zpožděním po jeho předchozí vládě. Míří

na voliče, kteří nechápou zpoždění opatření a hospodářský cyklus vnímají přes cenu buřtů. Nevnímají makro příčiny zdražování, jim stačí jednoduchá věta. „Volič medián“ se tomu říká. Problém u této kampaně nenastává ani s měřením, protože voliči, jež tato kampaň osloví, neposkytují žádnou zpětnou vazbu prostřednictvím internetu. Vnímají však influencery ve svém prostoru (TV, Blesk a iDnes) Správný nestranný názor jistě zajistí průzkumy Semantic Visions a podobných.

Semantic Visions se spoléhá na granty, prostředky od ministerstev a politických stran a politiků. Jedním z úspěchů firmy bylo získání grantu v hodotě 250 tis. USD v oblasti bezpečnosti obyvatel a odhalování desinformací.

Technologie Semantic Visions bývala primitivní, na míru zákazníkovi psané skripty v Javě, které neměly znovupoužitelnost u jiné firmy. Technický koncept oproti profi nástrojům rozpačitý. Ve světě se technologie monitorování kyberprostoru a odhadování chování obyvatelstva vyvíjí jinými směry, jeden z nich pro odhalování epidemií nebo nepokojů obyvatelstva ještě dříve, než nastanou, například realizovala Izraelka Kira Radinsky.

I přes relativní technologickou zaostalost měli Semantic Visions historický úspěch. Analyzovali dopad témat volební kampaně a provedli Babiše k volebnímu vítězství. Průzkum veřejného mínění to nebyl, spíše analýza jak kdo o Babišovi a ANO píše. Vytěžovali tisk a sociálních sítě. Počítali pozitivní a negativní zmínky a hodnoty vynášeli za každý den do grafu. Sledovali trendy. Soustředili se na ukazatele: jak často je politik zmíněn a zda je sentiment (významový nádech) zmínky negativní, neutrální nebo pozitivní.

Technicky na to šli takto: naprogrmaovali si v Javě algoritmus, který uměl dělat frekvenční analýzu, tj. kolikrát se sledovaný politik (Babiš, Filip apod.) v textu vyskytuje a zda v blízkosti pozitivních nebo negativních slov. K tomu sloužily slovníky pozitivních a negativních přídavných jmen a příslovcí. Blízkost pozitivních nebo negativních deskriptorů lze naprogramovat jednoduše. Ostatně vyhledávače Google, Altavista, Bing a další, umožňovaly kdysi používat tzv. „proximitní operátory“ např. Near() a Around() i běžným uživatelům. Dnes tyto možnosti nejsou běžně dostupné takže to vypadá trochu jako kouzlo.

Vyhodnocování sentimentu ale moc spolehlivě nefungovalo. A protože jsme v ČR tak je téměř vše co se napíše negativní, takže nemá smysl rozlišovat negativní a pozitivní zmínky, ale stačí sledovat jen počet zmínek. Ve výsledném grafu preferencí nasbíral například komunista Filip několik zmínek pozitivních a desítky zmínek s negativním sentimentem (vyskytl se blízko negativních výrazů) takže jeho “kolečko” v grafu Semantic Visions vykreslil převážně červené (převažující negativní sentiment). Politiků s několika desítkami zmínek pozitivními, neutrálními nebo negativními byla většina. Babiš nasbíral za totéž období ale stovky zmínek (také vesměs negativních) a zcela se od ostatních utrhl. Ocitl se v grafu zcela mimo shluk všech ostatních politiků. S probíhající kampaní se jeho náskok udržoval nebo zvětšoval. Časem sbíral téměř výhradně negativní sentiment a snahou týmu bylo identifikovat vztah tématu a počtu zmínek, který ukazoval jaká témata aktuálně zabírají nevíc na zvyšování počtu citací Babiše. Zní to triviálně, ale toto rozchodit není snadné a umět interpretovat výsledky měření také ne. Museli texty z médií plošně rychle vytěžovat. Dnes si na to koupíte produkty od Apify nebo si něco naprogramujete za pár hodin sami v Pythonu, tehdy to museli sami naprogramovat od nuly. Tahat copyrightovaná data z webů navíc je právně na hraně. Nicméně tehdy neexistovaly příliš sofistikované obrany webů před plošným vytěžováním, jako je tomu dnes.

Následně nad získanými daty provedli onu sémantickou analýzu. Tehdy nic nefejkovali. Babišův volební tým si platil drahé Semantic Visions a vyplatilo se. Chtěli být vidět, byť v negativním kontextu. Počtem zmínek ANO ujelo soupeřům o parník. Volili témata, která náskok maximalizovala. Jak primitivní, ale jak účinné. V následujících volbách ANO vyměnilo Semantic Visions za levnější agenturu, a nevyhráli. Možná to ale nesouvisí.

V Semantic Visions není také vše jak bývalo. Bývalý technický ředitel pracuje pro velkou konzultantskou firmu. Každý na vrábeloviny nemá náladu. Lidé, kteří mají mentální kapacitu a chtějí dělat pro svět něco pozitivního časem pochopili a odešli. Odchodem schopných lidí zřejmě i další vývoj firmy ustrne a firma bude ztrácet technologicky i v oblasti interpretace dat. To však pro přežití nemusí vadit, stačí, pokud bude mít image nestranného pozorovatele, sosat dotace a může pracovat skrytě na zakázku kohokoli. Kdo se zajímá o statistické modely ve výzkumech veřejného mínění, ví, že pokud máte hodně dat, dokážete v nich najít "požadovanou" závislost, takže si výsledky i budou moci nějak obhájit.

Semantic Visions hledá peníze u politických stran, shání granty a také zakázky z ministerstev. Může být a použita k ovlivňování veřejného mínění ve volbách 2022? Pokud si uchovají image "nestranného datového vědce" Vrábela a nikdo tuhle habaděru nerozkope, proč ne? Výroky pana pana Vrábela, týkající se COVIDu, Vrbětic a dezinformací v ČR známe. Jistě makají na tématu války na Ukrajině, vnímání uprchlíků atd. Blíží se volby tak možná přibyde i americká základna.

Jak psal Ondřej Neff: „… Andrej Babiš rozpoutal bizarní billboardovou kampaň, kdy „tváře z lidu" sdělují obyvatelstvu, proč bylo „za Babiše líp". Kampaň je to bezesporu nápaditá, svědčí o tom fakt, že o ní každý mluví, většinou posměšně. Ale mluví." Neff má pravdu, Babišovu týmu nejde o to, aby se o Andrejovi psalo s pozitivním sentimentem. Podstatné je, aby se o něm psalo. To byl hlavní parametr hodnocení kampaně v jeho předešlých vítězných volbách a pokud bude mít vplební tým schopného datového analytika, Andrej to vyhraje znovu. Stačí rychle vyhodnocovat reakci tisku a posilovat populární témata, která se ujmou i v AB neovládaných médiích. Je to takový A/B Testing. Téma A má nižší odezvu, uděláme B.

Tovek

Jestliže Semantic Visions představuje firmu, která chce ovlivnit veřejnost, pak firma **Tovek** je její opak. Není vidět a neanalyzuje nás jako dav, ale jako jednotlivce.

S Tovekem je od počátku spojen pan Tomáš Vejlupek. Spolupracuje s komerčními subjekty jako jsou banky, telekomunikační firmy a další korporace, umí to ale i se státní správou, včetně bezpečnostních a informačních složek. Dodává technologie a školení státním analytikům, sama firma se na analýzách dat zřejmě přímo nepodílí. Tovek poskytuje IT nástroje pro plošné sledování internetového prostoru a umí je efektivně propojit i s firemními daty, v případě státu pak s daty agendových informačních systémů. Řešení u komerčních subjektů netřeba popisovat, jak si například vaše banka vytěžuje data o vás jako o klientovi je její věc a je to myslím akceptovatelné, všichni s tím někde dáváte souhlas a je jedno zda mají nástroj Tovek Server nebo nějaký jiný komerční produkt. Problém pro řadu lidí nastane v možném využití Tovek technologie v monitorování života jednotlivce. Pro pochopení dopadu na vás jako čtenáře Dfensu nebo přispěvatele do diskusí na webu, je nutné se podívat na to, co Tovek nabízí a jak efektivně vás dokáže vytěžit.

Vznik Toveku se datuje do doby předgooglovské, kdy internetu kralovala Altavista nebo Seznam. K založení firmy se pojí zajímavý příběh, pár nadšených ajťáků provedlo reverzní engineering kódu produktu Topic od společnosti Verity. Údajně na IT výstavě předvedli užaslým zástupcům firmy Verity funkční verzi jejího vlastního produktu Topic, s vlastními úpravami. Firma Verity jim pak svěřila na několik let české zastoupení. Časem si Tovek vytvořil vlastní řešení, vycházeje z Topicu. Dnes je původní Verity – Topic součástí databázového řešení Oracle, který firmu Verity koupil. V Oraclu najdete tento nástroj jako jednu z mnoha voleb formulace dotazu do databáze. Moderní Tovek nástroje obsahují řadu příkazů, kderé se jinak píší leč chovají se podobně jako ty původní v Topicu. **Tovek využívá postupy pojmového vyhledávání**, hledá témata (anglicky topic) odtud

název původního produktu.

Pan Vejlupek je bezesporu vizionář, tlačil vývoj v českém prostoru vlastní cestou. Snaží se využívat AI a zřejmě věří, že činí dobro. Technologicky je jádro Toveku zastaralé a AI jako doplněk začíná být nutný prodejní argument. Nosný produkt Tovek Server se svým ekosystémem a schopností využívat moduly třetích stran, je snadno integrovatelný do IT systémů instituce, která si ho pořídí. V porovnání s nablýskanými produkty světových firem působí sice jako parní stroj, ale státním institucím na nás stačí parní mlátička, která udělá tutéž práci. Silná stránka Toveku je právě jeho jednoduchost, tvorbu pokročilých reportů (kombinujících několik zdrojů dat a různé řezy daty) zvládne po několikadenním školení i průměrný datový analytik ve státních službách. Tovek mu poradí, jak systém napojit na datové zdroje a dále je to na něm. Pro Tovek je orientace na stát dobrá, u státu finanční „zdroje jsou".

Technicky se Tovek soustředí na zpracování textových dat a řeči. Proto spolupracuje s firmami jako Retia (www.retia.cz) a Phonexia (www.phonexia.com), dodavateli modulů pro převod (telefonních i přímých) hovorů do textové podoby. V textové podobě hovoru se lze snadno orientovat, například nahrané a do textu převedené telefonní hovory za celý rok můžete vyhodnotit bez náslechů na jedno kliknutí během pár vteřin. Tovek nabízí řadu vymazlených analytických nástrojů od dodavatelů.

V souvislosti s Phonexia, je zde jedna čerstvá zajímavost z května 2022 – do této soukromě vlastněné brněnské firmy nastoupil bývalý ředitel Red Hatu a má za úkol firmu akcelerovat. Je to sekáč, „ten se nezakecá". Software od Phonexie umí rozpoznávat hlas, umí identifikovat mluvčí a přeést mluvené slovo do textu a prohledávat audio nahrávky. Firma spolupracuje například s Interpolem, s fimami T-Mobile, Innogy nebo Telefónica. Nejsou sice technicky tak daleko jako izraelci, ale na ČR je to kvantový skok.

Tovek se soustředí na práci s textem, a protože lidi toho víc namluví, než napíší, od firem i od státu roste poptávka vyhodnocovat co říkáme do telefonu, co se nasnímá na přepážce atd. Technicky to funguje výborně. Pokud existuje nahrávka telefonního hovoru „stereo", kdy volající mluví například na levém a volaný na pravém kanálu, získá se vysoce spolehlivý přepis. U mono záznamu nebo záznamu od přepážky spolehlivost výrazně klesá, zvláště pokud mluví více lidí přes sebe. Analytik z textu vytěženého z hovorů pak, v připraveném reportu, zjistí kde jste hovořili o konkrétním tématu (např. uprchlíci z Ukrajiny), o konkrétním člověku, konkrétním produktu či službě, a také v jakém kontextu (schvaloval jste, neschvaloval jste). Řeč po převedu do textu analyzuje Tovek z hlediska „významu". Pozná tak opravdu význam toho, co říkáme a nepotřebuje k tomu nevyzpytatelnou AI.

V komerčním telefonickém provozu Tovek nástroje zjišťují, zda v hovoru operátor použil sprosté slovo, zda volající řekl slovo žaloba, právník, soud, končím s vámi apod. Sleduje se automatizovaně kvalita obsluhy, například zda operátor skákal do řeči volajícímu nebo zda uvedl na začátku hovoru zákonem předepsanou formulaci, že hovor bude monitorován apod. Za neuvedení mohou být sankce ze strany regulátora takže je v zájmu firem toto vynucovat a plošně sledovat, operátoři proto tyto otravné formulace opakují. Pokud něco chcete na callcentru docílit, například aby váš případ předali seniornímu pracovníkovi k řešení, a nejen levnému brigádníkovi v ranní směně, který maximálně do systému zapíše ticket s váším požadavkem, zvyšte si prioritu obsluhy sami. Pečlivě vyslovte (nebo napište) slova „žaloba, právník, budu si stěžovat, ERU, ČTU, ČOI" apod. Vyplácí se slušnost a srozumitelnost. Čekejte, že se během několika hodin ozve firma zpět a začne váš požadavek kompetentně řešit. Mají KPI na kvalitu obsluhy a také negativní tisk si firmy nedovolí riskovat. Velké firmy mají zmíněnou datovou analytiku na všech obslužných kanálech, a to včetně monitoringu volání na mobilní telefony osobních bankéřů atd. Pokud vám dá bankéř svůj osobní mobil, věřte, že před přijetím telefonátu od vás zmáčkne v aplikaci na mobilu potvrzení zda jde o soukromý hovor (nenahrává a neanalyzuje se) nebo pracovní hovor (nahrává se a vyhodnocuje se). Mimochodem: dávali jste souhlas bankovní aplikaci s přístupem k telefonnímu seznamu a ke zprávám? Na trhu se

před pár lety objevilo zadání od středně velké banky, která požadovala po dodavateli e-bankingové aplikace aby prošel lokálně uložené zprávy v mobilu a našel klíčová slova ukazující, zda klient dostává výzvy k zaplacení účtů po splatnosti. Asi by se divil proč mu banka nechce poskytnout kreditku. Je to sice proti regulaci ČNB, schvalovací mechanismus musí být zdokumentován, ale management s tím neměl problém. Pozor: toto nedělá Tovek, jde jen o podobné téma, vytěžování textu.

Nyní zpět k Toveku. Ve státní službě má analytik za úkol sledovat právně závadné téma, obvykle ve spojení s nějakým člověkem, místem, firmou, uživatelským účtem apod. To, že dnes téma není závadné neznamná, že bude nezávadné v budoucnu. Pěkná vlastnost Toveku je, že si analytik téma rychle vyhledá, přečte si převedený text hovoru a reportované prohřešky jedince si může rozklikat až do úrovně konkrétního hlasového záznamu každého jednotlivého hovoru a může si je libovolně přehrávat. Z kontextu pak vymyslí, jak na zjištění reagovat. Hledáním v textu jde rovnou k věci, přepne se přímo do té části hovoru, kde je zmíněno zájmové téma, zájmová osoba, věc, místo nebo téma. Analytik si pohodlně propojí přepis hovoru, hlasový záznam a volajícího. Zjistí i jak dlouho ten člověk telefonoval, pokolikáté, z jaké lokality, komu atd. Podezřelé nemusí být jen pravidelné hovory z registrovaných čísel, ale i nahodilé hovory nově se objevivších několika předplacených čísel v určité lokalitě. To je typický vzor chování zločinců, seženou si předplacená mobilní čísla a přístroje na jedno použití a pak se v nějaké lokalitě objeví jeden pár hovorů mezi takto nově zaregistrovanými čísly. To je samo o sobě zajímavý spouštěč pro vyhodnocování, protože odporuje obvyklým vzorům chování. Policie si pak může propojit data z kamer v dané oblasti, takže lze zjistit kdo a čím kam přijel atd.

Moduly analýzy řeči dokáží zjistit, zda člověk s vysokou pravděpodobností lže, je ve stresu apod. Vyjet si pak statistiky jakéhokoli typu hovorů je jen otázka času věnovaného na sestavení příslušného reportu a přístupu k dalším obohacujícím datům. U státu opět platí, že „zdroje jsou“. Ty datové.

Jak Tovek zjistí téma hovoru a význam toho, co napíšeme?

Využívá dotazovací jazyk odvozený od zmíněného jazyku Topic. Pro každé hledané téma musí být navržen tzv. „pojmový strom“, což vyžaduje na začátku trochu práce a oborových znalostí. Pojmový strom napíše odborník na danou oblast. Strom má větve, na nichž jsou navěšena slova. Tato slova umí program skloňovat a časovat a doplňuje je o foneticky podobné výrazy. To se hodí pro analýzu řeči kdy mnohá slova podobně znějí. Jednotlivým slovům i celým větvím pojmového stromu lze přiřadit váhy slov. Váhy slov, a větví stromu, se násobí sčítají podle toho, jak moc se podobají analyzovanému záznamu řeči nebo zprávy. Vyšší souhrnná váha (score) znamená vyšší relevanci vůči definovanému dotazu. Existují i další možnosti jak zvýšit přesnost hledání, například v textu novinového článku lze definovat vyšší váhu tomu co je tučně, v nadpisu nebo v souhrnu, které každý čte.

Pojmový strom přinášel oproti holé booleovské logice (AND, OR, NOT) vyšší přesnost a úplnost vyhledávání. Pokud google kdysi dosahoval přesnosti cca 20%, pojmové vyhledávání v téže době dosahovalo 40%. Přesnost a úplnost indikují, že ve výpisu výsledků dotazu uživatele jsou u přesného algoritmu uvedeny na začátku výpisu nejrelevantnější výsledky, nejsou přitom uvedeny nerelevantní výsledky. Úplnost ukazuje, kolik existujících dokumentů sysém nalezl a kolik vynechal. Těch 40% se zdá málo, ale není. Pokud porovnáme to, co dnes google vrátí na váš dotaz, a co tušíte, že někde je ale google to prostě neukáže ani na sté stránce, ukazuje se, že je daleko od 100% pokrytí a přesný rozhodně není. Zkuste jiné vyhledávače a budete překvapeni zkreslenými výsledky. Technologická nedokonalost vyhledávání je korunována filtrováním toho co google poskytne v našem überkorektním světě. Něco v CZ doméně vůbec neukáže, a navrch vše upraví pro vás jako uživatele s určitými „preferencemi“, které si o vás sleduje napříč zařízeními. Zkuste si yahoo, bing nebo DuckDuckGo a uvidíte o kolik je svět pestřejší, než co vám servíruje google.

Tovek zmapuje obsah počítače než řekneš „borůvkovej koláč“

Tovek nástroje lze použít pro rychlou úvodní analýzu zabavených počítačů, datových nosičů, e-mailových účtů, logů z diskusí předaných provozovatelem serveru, dat vytěžených z diskusí pomocí webscrapingu, z logu komunikace za poslední 2 roky exportované z WhatsAppu atd. Tam může analytik ve státních službách získat data o vás, o rodině, o kamarádech, o známých, o obchodních partnerech, o vašich názorech a o vaší činnosti. Extrakt mailové komunikace nebo zpráv z whatsappu si někdo s uživatelským oprávněním uloží do dlouhého textového souboru, v němž se Tovek nástroje rychle zorientují. Pokud má výpis alespoň nějakou strukturu, například časové značky nebo adresáty, mailové adresy, telefonní čísla, Tovek si automatizovaně vytvoří asociace mezi daty, lidmi, místy, tématy apod. a pracuje s daty v podobě pohodlné rychlé relační databáze. Občas to chce nastavit importní filtry, ale při druhém použití na tentýž datový zdroj je to rychlé a pohodlné. V praxi existují případy, kdy se analytikovi dostane do rukou semistrukturovaný datový zdroj, v datech může být i díky nekonzistenci sběru dat v čase problém s měnícími se formáty nebo strukturou, nebo ten kdo dělal extrakt je prostě prase a udělal po sobě tři extrakty pokaždé s trochu jiným dotazem, takže se to pak musí růčo vyčistit, nicméně v praxi nebývá třeba si na tyto věci brát nástroje jako splunk nebo podobná děla. Telekomunikačních operátoři mají nastaveny standardní datové modely a ty nemění.

Automatická detekce závadných témat na tvém disku

Automatizovaná detekce závadných témat definovaných odborníky na všechny možné otázky trestního a jiného práva reálně velmi dobře funguje a lze ji provést na jakýchkoli strojově čitelných datech, i komprimovaných (včetně slabě zašifrovaných archivů ZIP apod.).

Z obrazových dat lze také automatizovaně číst obsah, jen to trvá déle, využívá se automatické OCR s podporou AI postprocessingu. Dříve dělal analýzu takového zdroje dat analytik dny nebo týdny. Dnes několik GB dat na disku nástroj přechroupe, než se analytik vrátí z oběda, obsah pěkně zaindexuje (zpřehlední pro vyhledávání) a tak v záznamech lze rychle hledat co je libo – místa, adresy, lidi, firmy, telefonní čísla, mailové adresy a další souvislosti v podobě klíčových slov a celých témat.

Protože Tovek umí i generovat sítě vazeb, vytvoří analytikovi volně proklikávatelnou pavučinu. Co dříve analytik dělal měsíce, dostane bleskově v interaktivní formě a může si obohatit svou analýzu vizuálním propojením subjektů a témat, kvantifikovat síly vazeb a tyto graficky znázornit v podobě různých sítí. Dozví se, s kým sledovaná osoba často mluvila nebo si psala, a s kým nahodile. Report je ale jen tak dobrý, jak dobrá jsou vstupní data. Smyslem analýz slidila je data propojovat, obohacovat. Do reportu tak může připojit i další zdroje dat a stát zdroje má jak víme. Nejde jen o Základní registry zapojené do eGona, ale i o další agendové informační systémy, které evidují vše co jim ukládá zákon a o kterých většina lidí nemá tušení.

Základní registry (ZR) eGovernmentu ČR

Analytik jde často po jménech firem, osob, míst a tématech definovaných pojmovými stromy. Za roky existence Tovek produktů existuje databáze těchto významových stromů. Tak systém detekuje lidi, podle databáze obyvatel nebo osob (právnických) a umí pracovat s daty z jakýchkoli databází, má na to připravené databázové konektory. Uživatelé Toveku mohou mít přístup k datům ZR nebo i k jejich extraktům. ZR nejsou vždy aktualizované v reálném čase, dokonce se tam promítají změny i po několika dnech. Nečekejte žádná spektakulární řešení typu amerického systému Palantir.

Představte si tento případ: co když bude existovat oprávněný zájem, aby někdo v naší zemi měl přístup ke všem datům která jsou technicky dosažitelná prostřednictvím ZR a dalších agendových informačních systémů jakéhokoli ministerstva nebo jeho podřízené nebo spolupracující organizace?

Jak by se to dalo udělat? Když integrovat data v nějakém ministerstvu, snad s výjimkou vnitra, je nadlidský úkol a většinou to dobře nefunguje? Možná by to šlo takto: existuje jeden, poněkud utajený pátý Základní registr tzv. Registr práv a povinností (RPP). „Jeden, co vládne všem“. Přiděluje uživatelům práva pro přístup k dílčím datům a přístupy k datům eviduje. Chodí vám do datovky sjetiny, kdo se na vás díval? Tak to je jeho výstup. Jde o bazální ochranu, aby si úřednická krysa žijící z eráru jako suvenýr neodnesla domů celou ČR na jednom disku. Otázka je, zda existuje někdo ve státní doméně, kdo má nelogovaný přístup ke všem datům? Neumím si představit, že by architekti systému toto nemuseli navrhnout. Takový backdoor. K jakým datům a čemu mohou mít superprivilegovaní uživatelé přístup a kdo je pak kontroluje? Soudě podle dostupných rozhovorů s architekty eGONa, je systém navržen se spoustou kompromisů a nemám pochybnosti o tom, že pokud se najde zdůvodnění, aby nějaký uživatel nebo IT systém měl v RPP povoleny nelogované přístupy kamkoli, tak se to využije. Technicky lze tato data dala analyzovat a zobrazovat Tovek enginem nebo v čemkoli jiném. To už je jedno.

Pokud by tomu tak bylo, dle dostupného popisu architektury ZR pak budou k dispozici kromě dat občanů a právnických osob i data vlastněných a provozovaných vozidel, vazby z RUIANu, Katastru nemovitostí popisující vlastnické vazby, adresní místa, samozřejmě lze přihodit data finančních úřadů, sociálky, vlastněných vozidel psaných na konkrétní majitele atd. Navrch přidejte data z veřejného prostoru, kde o sobě lidé prozrazují detaily s naprostou lehkomyslností. Zde malý tip: poskytujte státu co data v PDF jako torky, obrázky, a pokud možno blbě naskenované a pootočené. Pokud nevyžadují jako doprovod elektronickou větu, s obsahem si neporadí. Jde zejména o kopie kupních smluv na nemovitosti, výroční zprávy firem apod. Kromě přepisu telefonických hovorů, SMS a zpráv z instant messagingu a dalších zdrojů jsou ZR další zdroj dat pro kohokoli s příslušným oprávněním, a je možné, že i bez jakékoli kontroly.

Pokud máte strach o své soukromí, zapněte si na mobilu pro svou identifikaci výhradně PIN. Pokud ho otevíráte biometricky otiskem prstu nebo pohledem do kamery, zamyslete se, jak dlouho bude trvat útočníkovi / zájemci o vaše data, než vás přiměje mobil odemknout a jak na to asi půjde.

Tovek vám rozumí – chápe, co říkáte

Úspěšnost převodu řeči na text bývá přes 80 i 90%, pokud jde o telefonát z normálně hlučného prostředí. Je problém, pokud je 20 ze 100 slov špatně rozpoznáno? Vžijte se do role slídila, který poslouchá hovory a na 1 hovor v délce 5 minut spotřebuje 4 minuty na poslech (rychloposuvem) a pak pár minut na přepis. Pokud by dokázal s Tovek nástroji najednou převést byť jen 60% obsahu hovorů správně, je to obrovský skok v efektivitě monitorování komunikace proti dřívějšku. Poslech je stále zapotřebí, ale jen v pasážích, které nebyly korektně rozpoznány a algoritmus to označil buď jako chybné rozpoznání nebo jako nejasné slovo, které zní podobně jako jiná slova, v tom případě nabídne modul náhradní významy. S použitím oborových slovníků úspěšnost roste přes 90%, takže zde narostla efektivita šmírovací práce k dokonalosti. Člověk sice rozumí skoro všemu, ovšem rozdíl ve výkonnosti stroje vs. člověka je zhruba výkonnost stroje. V plošném monitorování stát nebo firma nemusí rozumět všemu, stačí zachytávat signály a doplňovat si trendy. Takže pokud do vytěžených témat doplníte trendovou analýzu, můžete si jako firma monitorovat například zájem o výrobky nebo sentiment pojící se k produktu. Stát si může průběžně monitorovat radikalizaci společnosti a to až na úroveň konkrétního příspěvku jednoho každého člověka. Co bude označeno za radikální ponechme s důvěrou na Piráty, Zelené a spol.

Technicky: pro analýzu obsahu řeči využívá Tovek přepisy získané z integrovaných modulů od firem Retia nebo Phonexia, možností je více. Obdobně se těží data z grafických podkladů jako jsou OCR dokumentů, fotek apod. opět s pomocí specializovaných modulů. Videa zatím zřejmě nejsou využívána, ale s nárůstem trénovaných AI systémů se můžeme dočkat rychlého přepisu toho, co se mihne na jakémkoli videu.

Na každého z nás se vede složka – zavedli jsme si je sami a vytváříme si sami na sebe kompro

Pokud státní analytik vytěžuje reakce v diskusi na téma s trestněprávní dimenzí, bude se zajímat i o atributy příspěvku, jako je IP adresa uživatele. To, že je dlouhodobě evidována IP adresa, resp. digitální otisk zařízení a další atributy přispěvatelů na servery, je vyžadováno zákonem. Lidé bezelstně píší do diskusí na iDnes a milionu dalších. Vsadil bych se, že právě iDnes je vytěžován plně a vše může a bude jednou použito proti pisatelům. To, že váš komentář je dnes legální, nezaručuje, že nebude zneužit v budoucnu. Každý si tak zakládá a vede si složku sám na sebe. Takže gratuluji všem, co si tam udělali ofiko účet a měli potřebu něco sdělit světu, dokonce i pokud něco lajkovali nebo dislajkovali. Ušetřili šmírákům práci se svou identifikací. Tyto věci budou i za deset let použitelné proti nim. Složka dnes není formálně vedena s labelem Josef Vohnout, ale na Josefa Vohnouta se dá zpětně sestavit podle potřeby. Efektivní, flexibilní, levné. To, že stát operátorům nařídil, že musí evidovat logy k hovorům 6 měsíců, je irelevantní. Weby vytěžují desítky firem (viz např. Semantic Visions) a další internetové služby, o těch státních nevíte, ale běží a servery tam vesele cvrlikají již roky.

Monitorování hovorů v reálném čase

Tovek uměl již před lety převádět řeč na text v reálném čase, náročnost převodu hlasu na text v reálném čase byla cca stejná jako ze záznamu, na 1 hovor bylo třeba 1 jádro procesoru, časově seděla cca doba zpracování s reálným časem hovoru, zpoždění bylo pár vteřin. Není to tedy optimální pokud chcete odposlouchávat vše, co se kde v ČR řekne, ale blíží se čas kdy to bude technicky možné v reálném čase. U záznamů bych odhadoval, že lze procházet a vyhodnocovat zrychleně. Dnes by u hovorů v reálném čase mělo běžně fungovat, že u vybraných čísel jede dohled 24×7 se zanedbatelnými náklady na správu, elektřinu a úložiště. Plná automatika.

Zmíněné moduly uměly již dříve přepsat hovorovou češtinu na text s přesností 60% bez tréninku. Tréninkem lze vyhnat úspěšnost přepisu k 90% a výše. Využívají se k tomu oborové korekční slovníky, typicky jsou nasazeny například v bankovnictví a pojišťovnictví. Důležité je z technického hlediska rozlišení stran volající a volaný, takže jak jsem již psal výše, hovor se zpracovává „stereo“, kdy každý levý a pravý kanál reprezentuje různé strany hovoru. Pokud mluví více lidí například v telekonferenci, tak nastává problém zjistit kdo co řekl, ale pokud nemluví lidé jeden přes druhého, vychází přepis čitelně a hlavně se získají snadno prohledatelné hromady textů.

Analytik ve státních službách ví od telefonních operátorů u většiny čísel kdo s kým mluví, případně ví, že neznámé číslo mluví s někým koho již znají nebo se dokáží k jeho identitě dostat. Cesty jsou. Analytik rozhodně nepotřebuje mít u hlavy sluchátko, přehraje si tak nanejvýš nesrozumitelnou nebo jinak zajímavou část rozhovoru, kterou automat nerozluští nebo kde nabídl fonetické alternativy a kontext vyšší pozornost vyžaduje. Fulltextově tak pohodlně vyhledává v přepisech hovorů pana Vohnouta a jeho širokého okolí, přičemž Tovek mu sám pěkně vytváří shluky témat, která sám detekuje. Vypadá to taková ptákovina, ale pro rychlou orientaci to stačí a někdy člověk kápne na zajímavé vazby – není nad obrazovou reprezentaci dat. Tovek umí také odfiltrovat nepodstatné, ať se jedná o často se opakující slova nebo naopak umí zvýraznit slova neobvyklá, unikátně použitá. Používá k tomu statistickou analýzu, která je zatím triviální. Ale nebojte se, pracuje se na řešeních pro analýzu významu textu, která jsou téměř dokonalá. Ta analyzují shodu s pomocí korpusů psané a hovorové řeči – viz www.korpus.cz, ten nabízí vedle psaného současného jazyka v rozsahu přes 4 milardy českých slov i soubory spontánního mluveného jazyka s obsahem přes 7 milionů slov plus open-source nástroje pro významovou analýzu textu.

Tovek se asi přímo nepodílí na vyhodnocování dat o nás. Poskytuje státu i komerčním subjektům nástroje a školí jejich uživatele na vytěžování našeho soukromí. Je otázka jak je to s dohledem nad státními zaměstnanci, kteří tyto nástroje používají, a jak jsou uplatňovány základní principy řízení přístupu k darům v Základních registrech.

Semantic Visions je příklad firmy, která je nástroj manipulace s veřejným míněním. Vyhodnocuje účinky toho co politik řekne a umožňuje ladit výroky politika podle situace. Podobných firem je více a **Semantic** Visions je již zřejmě díky technologické zaostalosti za svým horizontem. Po panu Vrábelovi sáhne Márův tým až bude potřebovat nějaké téma podepřít „nestrannými“ názory.

Obě firmy mají slabá místa zejména ve zpracování grafických dat, neumí vyhodnocovat streaming videa nebo videozáznamy, tyto oblasti jsou však pokryty jinými firmami.

Video záznamy z kamer na veřejných místech

V ČR exitují desítky AI orientovaných firem, z nich se některé účastní projektů a výběrek organizovaných např. vnitrem nebo policií. **Jedno z témat bylo ověření přesnosti a rychlosti zpracování dat z veřejných kamerových systémů. Šlo o detekci osob, například systém nakrmíte 2D fotkou zájmové osoby a tu musí systém poznat na pohyblivých záběrech u vstupu do objektu.**

Zájem je i o analýzu pohybu vozidel a posádek. Zdrojem jsou kamery na území Prahy, videa od PČR, MP, ŘSD z dálničních kamer a kamer na pražském okruhu atd.

Nebojte se, vše je legální a řízené ministerstvem, nemějte strach ze zneužití svých dat. Jde o vyšší bezpečnost v tunelech v Praze a o potlačování organizovaného zločinu. Zajímavé jsou i případy sledování návštěvnosti parkovacích míst před určitými budovami. AI dokázala identifikovat konkrétní vozidlo z různých úhlů, i když bylo vidět jen částečně a i když nebyla vidět RZ. Pro lidi je zajímavé, že AI si vybere nějaký deskriptor objektu a ten si dokáže zapamatovat a najít a uvede i procento jak moc si je identifikací jistá. Sledování v tunelech, sledování příjezdu a odjezdu aut vč. evidence RZ z

virtuálních parkovacích míst na území města nabízí možnosti sledování trasy jednoho vozidla a posádky kdekoli po území města i mimo ně. Člověk si řekne, že auto pozná podle typu, barvy, RZ, případně podle samolepky. AI pozná totéž auto nebo osobu i pokud se trochu natočí podle umístění různých záchytných bodů a vizuálních charakteristik. Pokud si je necháte prozradit, ukáže něco, co vůbec nevnímáte jako něco člověkem uchopitelného. Lidi AI pozná i poté, co si vymění oblečení, podle způsobu pohybu, vzoru chůze. Stačí k tomu dobré rozlišení videa.

Při nákupech se usmívejte

V české kotlině analyzuje obsah videa minimálně jeden obchodní řetězec, který je schopen vás na pobočkách od vstupu až po opuštění prodejen každou vteřinu několikrát vyhodnotit. Určí, zda jste muž, žena. Nebinární mají tentokrát smůlu a můžou si zajít stěžovat na informace. Pozná „to“ i váš věk, náladu, kam se koukáte atd. Zmapuje to vaši přesnou trasu po obchodě. Rozpoznat náladu, věk a pohlaví umí i vaše Raspberry Pi za tisícovku? Oni ale poznají kam se díváte s přesností na několik úhlových stupňů. Následující funkce sice systém nabízí, ale v těchto prodejnách se zřejmě nevyužívají: pozná, že jste vzali do ruky lahev i to zda jste ji vrátili do regálu zavřenou nebo jste lahev otevřeli a dokonce i zda jste se napili. Další funkce která už by mohla mít pozitivní odezvu u zákazníků je, že systém umí rozpoznat nehybné tělo, pád člověka, tj. situace kdy je třeba volat pomoc. Umí také poznat, zda držíte zbraň v pozici „střelec“. Ani to neměli zapnuté. Co však zkoušeli, je udělat jakýsi mystery shopping, změřit u regálu zda se jak dlouho se díváte do kterého fochu na který výrobek a to vyhodnotit. Je to sice objektivnější, než zaměstnat otrávenou pani, která si bude dělat čárky na papír co kdo bere do ruky, ale to vyhodnocení je drahý, navíc se musí spárovat se skutečně prodaným artiklem, aby to dávalo nějaký obchodní smysl. Agentury to ještě neumí, takže to byl takový sen pro lidi z marketingu, kdysi, když ještě měli motivaci něco dělat. Preventivně se ale při tlačení vozíku s nákupem usmívejte, zlepšíte si score loajálního zákazníka a dostanete třeba slevu na lahváč.

Toto řešení je nasazené i v jedné finanční instituci, „protože sekurita“. Data feed jde z fisheye kamery, která je v openspace instalovaná pod stropem. Sleduje vybraná pracoviště 360°. V zájmu ochrany zaměstnance. Podepsali souhlas s nakládání s osobními údaji zaměstnavatelem, a jde tu především o ochranu jejich zdraví. Jinak by se to nesmělo. Umí „to“ sledovat překvapivé detaily, jako jsou stupně volnosti kloubů ruky položené na myši. AI potvora má naučené lidské tělo, takže pozná i to, zda zaměstnanec kliknul jednou nebo dvakrát. Umíme automaticky měřit aktivní čas strávený v práci telefonováním, klikáním, nebo zíráním z okna. Vypadá to jako ptákovina, ale zde dnes již jsme.

Není to v rozporu s GDPR ani ochranou osobních dat

Systém neuchovává obrazovou podobu člověka, ani osobní data, ale jejich derivát, uloží si jen “vektor čísel”, digitální otisk. Z toho nelze zpětně zrekonstruovat přesný obraz člověka. Aniž by systém porovnával fotky nebo videozáznamy, pozná, že na novém záznamu je ten samý člověk, který byl před měsícem na jiném záznamu, nyní již smazaném. Kamera snímá a odvozuje ze vzhledu a pohybu unikátní popisné vzory, které nejsou pro nás rozpoznatelné, databáze si zaznamenává vytěžený digitální otisk a metadata jako místo, čas apod. Není problém videozáznam po uplynutí zíkonné lhůty pro jeho skladování smazat. Člověk je pro účely sledování dobře popsatelný a lze k němu vytvářet levně skladovatelnou sadu dat. Pro šmíráky ideál.

Obrana s rozumně vynaloženým úsilím zřejmě neexistuje

Obrana je individuální s ohledem na životní styla má omezený účinek. Můžete se zkusit anonymně pohybovat po městech, po internetu, po silnicích, ale je to vyčerpávající a často i neúčinné.

Zkuste se zamyslet, jak se opravdu anonymizovat když chcete poslat textový příspěvek do

diskuse, kterou monitorují?

Laik si zapne v Chrome anonymní režim, případně nějakou VPN a vymaže historii v browseru. znalejší s tím neztrácí čas, zaplatí si VPN a doufají, že nikdo nevynaloží dost úsilí aby je vytrasoval. Lidé často komunikují přes end-to-end šifrované kanály jako WhatApp nebo Telegram a doufají, že se jejich názory ztratí mezi ostatními nebo že nikoho nebudou zajímat. Paranoki si koupí bazarový mobil za hotové, v roušce s kapucí na hlavě. Vloží předplacenou SIM koupenou také za hotové. Zajde někam mimo kamery, kde je pokrytí mobilním signálem a skrytě odešlou zprávu prostřednictvím anonymní služby. Pokud bude zpráva delší, lze autora i tak vysledovat podle způsobu vyjadřování, psaní interpunkce a slov nebo jejich vazeb. Stačí mít k posuzované osobě jiné další texty, které prokazatelně psala a vzorek se s nimi porovná.

Obecně by obrana měla být proporcionální obsahu, takže nemá smysl vyšilovat, když si chci přečíst článek na dfensu. Pokud se ale rozhodnu někam něco napsat, musím vědět, že co napíšu již nikdy nevezmu zpět a bude to se mnou propojitelné.

Co bude dál?

Monitoring názorů lidí se přesune od izolovaných, mnohdy pilotních řešení do standardizovaného, legislativně podporovaného a státem dotovaného vytěžování populace. Monitoring end-to-end šifrovaných služeb je zadán přímo z EU, týká se služeb jako WhatsApp a podobných komunikačních kanálů a to nelze dělat manuálně, bude se možná dělat realtime a v rámci prevence plošně. V big datové oblasti jde o běžný postup, dat je moc, takže je nutno je zpracovat v reálném čase a ihned zahodit. Ex post to již nedává moc smysl. Stát to nenechá ani na komerčních firmách jako Facebook apod., bude to dělat sám. Nechá si udělat k příslušnému úložišti zpráv datový konektor a bude si prosívat co chce zcela bez zkontroly. WhatsApp není navržen jako Základní registry.

Během roku 2023 nám stát automaticky zřídí snad přes 3 miliony datových schránek. Ty budou „na fyzika“ a jediná cesta, jak se zachránit před zneužitím ze trany státu nebo firem či jednotlivců bude okamžitě se přihlásit a zakázat ve službě datových schránek příjem zpráv. Nebude možné nepřevzít doporučený dopis od souseda nebo od kohokoli kdo vás bude chtít buzerovat. **Datová schránka zajistí průkazné doručení obsahu v konkrétním čase. Nelze se na nic vymlouvat. Buďte proto rychlí. Zlí parchanti totiž rychlí budou. Schránku vám zřídí stát podle presumce, že jste počítačově gramotní. Důkazem bude, že jste se někdy přihlásili k jakékoli elektronické službě státu a je o tom záznam, propojitelný s průkazným ověřením vaší identity v tom daném případě.** Pokud máte datovku jako OSVČ nebo jednatelnebo statutár firmy, není o čem diskutovat. S počítačem umíte a budete se muset prokousat tím neskutečným marastem, který architekti a programátoři ve státních službách stvořili. Je to doslova k poblití, a pokud celý koncept výrazně nepřepracují, dojde na defenestrace. S onou presumpcí počítačové gramotnosti je to podobné, jako že důkazem že máte TV a rádio je to, že odebíráte elektřinu. Musíte sami aktivně říci ČT že televizor nemáte, jinak platíte. Tady je to podobně. Státnímu parazitovi se líbí používat presumpci viny, presumpci schopností, presumpci konzumace služby, objektivní odpovědnost majitele vozu apod. jsou dnes silně prosazované principy. ÚS ani soudruh Rychetský nás před tím nezachrání.

Změní se státní management v oblasti řízení eGovernmentu vč. DS a Základních registrů (tj vč. principů řízení přístupů k našim datům) přesune se z Ministerstva vnitra ČR pod Vládu ČR, zřejmě na základě tlaku Bartoše a fanatiků z řad Pirátů. Nemají zábrany. Ostatně před týdnem odstřelili v EU spalovací motory. Nyní v ČR makají na zrušení svobody (po) projevu.

ZDROJ