BI201K

Dojezd z minula

Jakub Harašta

Soukromí

- Nelze zasáhnout do soukromí bez souhlasu
  - Zákonné výjimky
  - Proporcionální posouzení

Zákonné výjimky

- Užití podobizny, zvukového nebo obrazového záznamu pro
  - Tiskové, rozhlasové, televizní nebo obdobné zpravodajství
  - Vědecký účel
  - Umělecký účel

Proporcionalita

- Kolize subjektivních práv – práva nejsou obecně „větší“ nebo „menší“
- Princip: momentálně hodnotnější právo musí převážit a musí se minimalizovat zásah do méně hodnotného

Test proporcionality

- Kritérium vhodnosti
  - Umožňuje institut omezující základní právo dosáhnout cíle?
- Kritérium potřebnosti
  - Lze cíle dosáhnout jiným opatřením, které by se nedotýkalo základních práv a svobod?
- Kritérium poměřování
  - Zvažování empirických, systémových, kontextových a hodnotových argumentů v kolizi stojících práv

Příklad kolize práv

- Zveřejňování platů zaměstnanců státní správy v odpovědi na žádost dle zákona č. 106/1999 Sb.
  - Právo zaměstnanců na soukromí – plat je důvěrná informace
  - Právo veřejnosti na informace – prostředky jdou ze „společného“
  - Řešení: např. zveřejňování platů zaměstnanců od náměstků výše nebo pouze nefixní složky mzdy

Příklad kolize práv II

- Zveřejňování údajů o členství soudců v KSČ
  - Právo soudce na soukromí – členství v politické straně
  - Právo veřejnosti na informace – pochyby o morálním profilu bývalých členů KSČ
  - Řešení: např. u soudce ustupuje soukromí ohledně členství v KSČ do pozadí.

Příklad kolize práv III

- Lidé jsou zvědaví – zveřejnění fotografie náhodné osoby, která dělá něco zvláštního, aby došlo k ukojení zvědavosti čtenářů.

  vs.

- Zachycení politika při podobné situaci se společností.

Příklady kolize práv IV

- Využívám pracovní mail pro soukromou korespondenci.
  - Právo na soukromí – ochrana soukromé korespondence
  - Právo vlastnit majetek / právo podnikat – využívám k tomu majetek zaměstnavatele
- Zákoník práce specifikuje, kdy lze sledovat komunikaci zaměstnance (obsah vs. hlavičky)

Zákonné omezení práva na soukromí

- Pouze a výlučně v zájmu ochrany demokratické společnosti nebo ústavně zaručených práv
  - Např. obecný zájem na ochraně před trestnou činností (uvěznění) nebo hospodářském blahobytu země (daně) nebo ochrana zdraví (věk obyvatel pro očkování)

Právo na soukromí v. osobní údaje

- Soukromoprávní vs. veřejnoprávní
- Restituční vs. Prevenční
- Soud vs. Úřad

BI201K

Výzvy soukromí v informační společnosti

Jakub Harašta

Co je „informační společnost“?

Entropie

- Pokud není organizující informace, dochází k entropii.
- Právo, zdravotní péče apod.

Informační společnost

- Rozšíření ICT
  - Výkon a dostupnost
  - Využití potenciálu k distribuci informací
- Změny v
  - Geografii a vnímání vzdálenosti
  - Mezilidských vztazích
  - Obchodních vztazích
  - Zábavě

Post-informační společnost

- Informace konstituují naše vnímání reality
  - Pokud SW vyhodnotí chování člověka jako riziko, vnímáme ho jako riziko
  - Zprostředkování ICT přímo ustavuje to, co vnímáme jako reálné

Jaké výzvy?

Nic neskrýváte – ničeho se nebojte

- Viz http://www.smbc-comics.com/index.php?id=4083

Co se o Vás dá zjistit?

- Facebook, LinkedIn
- Twitter, Pinterest, Instagram
- Gmail, Dropbox, Google Drive
- YouTube, RedTube
- Tesco, Lidl, věrnostní a slevové karty
- CCTV (venku, uvnitř)
- VPN, Eduroam
- Komunikační metadata

Čím Vás můžeme identifikovat?

- Chůze, hlas, sítnice, tvar obličeje
- Vaši přátelé a rodina
- Používání platební karty
  - Na základě čeho Vám banka zablokuje kartu?
- Vzorce v chování v domácnosti (smart grid, smart metering) i jinde (přihlašování na PC v pořadí služeb, omyly v heslech; „otisky prohlížečů“)

A když už jsme u toho, tak…

- Cílené používání slabého šifrování nebo backdoorů

Soukromí v. bezpečnost

- Všechno by mělo být přístupné zpravodajským službám, orgánům činným v trestním řízení, finančním úřadům (vč. FAÚ)

Data retention

Co je DR?

- Blanketní uchovávání provozních a lokalizačních údajů
  - Preventivní
  - Celoplošné
  - Do minulosti

Provozní a lokalizační údaje

- Metadata
- Provozní údaje
  - §90 ZoEK – údaje zpracovávané pro potřeby přenosu zpráv sítí el. komunikací nebo pro její účtování
- Lokalizační údaje
  - §91 ZoeK – údaje určující polohu telekomunikačního koncového zařízení uživatele veřejné služby el. komunikací

DR vs. odposlech

- Preventivní vs. konkrétní
- Celoplošné vs. striktně omezené
- Do minulosti vs. do budoucnosti
- Metadata vs. obsah

Kontroverze

- Narativ bezpečnosti – Efektivní nástroj využívaný při odhalování pachatelů širokého spektra trestné činnosti

  vs.

- Narativ soukromí – Bezdůvodné a neefektivní šmírování a špiclování běžných občanů

Kontroverze II

- Veřejný zájem na odhalování a vyšetřování TČ

  vs.

- Ochrana soukromí jednotlivce, ochrana telekomunikačního tajemství

Provozní údaj

- Kdy – kdo – s kým – jak dlouho

Lokalizační údaj

- Kde
- „V některých případech jsou (lokalizační údaje) cennější, než samotný obsah hovoru“
  - Jan Šubert (mluvčí BIS)

Proč DR?

- Harmonizace trhu
- Vymahatelnost práva
- Terorismus
  - New York 2001, Madrid 2004, Londýn 2005, Paříž 2015 (leden, listopad), Brusel 2016
- Kyberkriminalita
  - Anonymita vs. digitální stopy („Going dark“ dále)

Směrnice

- Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

Vývoj

- 21. 9. 2005 – návrh
- 14. 12. 2005 – souhlas EP
- 21. 1. 2006 – souhlas RM
- 15. 3. 2006 – vyhlášení v ÚV
- 15. 6. 2006 – žaloba na neplatnost
- 15. 9. 2007 – provedení
- 10. 2. 2009 – C-301/06
  - Formální přezkum před ESD

Cíl

- Zajištění dostupnosti údajů pro účely vyšetřování, odhalování a stíhání závažných trestných činů
- Harmonizace

Obsah

- Údaje k
  - Dohledání a identifikaci zdroje sdělení
  - Identifikaci adresáta sdělení
  - Zjištění data, času a doby trvání komunikace
  - Určení typu sdělení
  - Identifikaci komunikačního vybavení uživatelů nebo jejich údajného komunikačního vybavení
  - Zjištění polohy mobilního komunikačního zařízení

Provedení směrnice

- Účel – vyšetřování, odhalování a stíhání závažných trestných činů
- Přístup – poskytování pouze příslušným vnitrostátním orgánům v konkrétních případech a v souladu s vnitrostátními právními předpisy; nezbytnost a přiměřenost
- Doba – 6 až 24 měsíců

- 12/2008 – bulharský NSS
- 11/2009 – rumunský Ústavní soud
- 3/2010 – německý Spolkový ústavní soud

- Neproporcionální zásah do práva na soukromí
- Permanentní sledování všech občanů
- Absence podezření
- Nedostatečné procesní záruky
- Neinformování o přistoupení k údajům
- Nejasné vymezení doby uchovávání

  atd.

§97, odst. 3

- Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytování jejích veřejně dostupný služeb elektronických komunikací (…)

Kdo?

- PO/FO zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací
- ! Poskytovatel služby informační společnosti

Komu?

- Policie ČR
- Bezpečnostní informační služba
- Vojenské zpravodajství
- + Policie ČR předává zpravodajským službám, ministerstvu, Vězeňské službě, Celní správa a dalším orgánům Veřejné správy, je-li to nezbytné
- + pátrání po osobách
- + boj proti terorismu

Za jakých podmínek?

- K objasnění skutečností důležitých pro trestní řízení
- §88a odst. 1 TŘ

DR vs. odposlech

- DR (§88a)
  - K objasnění skutečností důležitých pro trestní řízení
  - Nemusí být kontrola ze strany SZ
- Odposlech (§88)
  - Zvlášť závažný zločin nebo jiný úmyslný trestný čin k jehož stíhání zavazuje vyhlášená MS; významné skutečnosti pro trestní řízení, které nelze získat jinak; na návrh SZ soudci; ex post informační povinnosti

Návrh – DR přes ÚS

- Stížnost vypracovávána od počátku DR
  - IuRe (Jan Vobořil)
  - Skupina 51 poslanců (Marek Benda)

Porušená ustanovení

- **Čl. 7 odst. 1 – nedotknutelnost soukromí**
- **Čl. 10 odst. 2 a 3 – ochrana před zasahováním do soukromí**
- **Čl. 13 – telekomunikační tajemství**
- Čl. 8 Úmluvy
  - Porušení zásady proporcionality

Argumentace

- Shromažďování údajů o komunikaci jako zásah do soukromého života
- Závažnost a rozsah zásahu do práva na soukromí
- Legitimita cíle a přínos zásahu do základních práv
- Nebezpečí zneužití uchovávaných údajů

Rozhodnutí ÚS – 24/10

- „Směrnice o data retention… ponechává České republice dostatečný prostor pro její ústavně konformní transpozici do domácího právního řádu.“ (Pl. ÚS 24/10 ze dne 22. 3. 2011)
- Proporcionalita?
  - Nejasné vymezení orgánů, nedostatečné záruky
- §97 odst. 3 a odst. 4 zákona č. 127/2005 Sb. se ruší

Rozhodnutí ÚS – 24/11

- Zrušení §88a
  - Příliš mnoho oprávněných subjektů
  - Příliš nízko nastavený práh pro přístup k informacím

Úpravy

- Taxativní výčet oprávněných orgánů
- Úmyslné trestné činy
  - 3 roky
- Trestné činy (vyhlášené MS) + taxativní výjimky
- Zdůraznění principu subsidiarity
- Příkaz státního zástupce
- Povinnost zlikvidovat data neobnovitelným způsobem

„Nová“ DR

- Ústavně konformní
- Vyhláška č. 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů

Kdo?

- Telefonní operátoři, poskytovatelé připojení
- Spor o poskytovatele veřejných wi-fi připojení
- 99,5% žádostí za 10 největšími subjekty

Co?

- Typ připojení
- Identifikátor uživatelského účtu
- Identifikátor zařízení uživatele služby (MAC adresa, telefonní číslo u dial-up připojení)
- Datum a čas zahájení a doba trvání přístupu k internetu
- Síťový identifikátor zdrojové strany komunikace (IP adresa, číslo portu)

Padá Směrnice… něco si přej

- SDEU ve spojených věcech C-293 a C-594 (populární název *Digital Right Ireland*)
- 8. duben 2014
- TL;DR – Směrnici 2006/24/ES si okamžitě strčte do špic!

Důvody

- Zásadní narušení čl. 7 a 8 Charty, které nebylo náležitě odůvodněno podle čl. 52 odst. 1
- Proporcionalita
  - Cíl je legitimní a zvolený nástroj je vhodný, ale…
  - Rozsah – příliš velký
  - Limity – nedostatečně specifikované
  - Doba uchovávání – nedostatečně specifikovaná

Důsledky (zjednodušeně)

- Blanketní uchovávání provozních a lokalizačních údajů na úrovni unijního předpisu již není možné

Důsledky

- WP29
  - Je nutné jednoznačně instruovat státy, co mají dělat
- EU
  - Meh….

Přej si něco národně…

- Slovensko
  - 23. 4. 2014 – pozastavení účinnosti
  - 29. 4. 2015
- Rakousko
  - 27. 6. 2014
- Slovinsko
  - 3. 7. 2014
- Rumunsko
  - 8. 7. 2014

Co dál v ČR?

- Blanketnost – porušení Charty
- Profesní tajemství – porušení Charty
- Ex post informování dle §88a odst. 2 TŘ, ale §88a odst. 3 TŘ – porušení Charty?

Co dál v ČR? II

- Nebudeme vědět, dokud se k problematice nevyjádří Ústavní soud
- Osobně: měl by to udělat co nejdřív
  - Náklady operátorů
  - Již shromážděné důkazy

„Going dark“ narativ FBI

FBI v. Apple

- Prosinec 2015: útok Syeda Farooka a Tashfeen Malik za sebou nechává v San Bernardinu 14 mrtvých
- Únor 2016: soud předběžně přikazuje společnosti Apple pomoci s odblokováním zajištěného telefonu. Vydáno na základě All Writs Act (1789). Nakonec soud 29. 2. 2016 vydání writu odmítá.
- Březen 2016: FBI zvládla telefon odblokovat sama (resp. za pomoci třetí osoby – spekulace směřují k izraelské společnost Cellebrite)

Google?

- 2015 – státní zástupce v New Yorku prozradil, že Google má možnost na dálku resetovat heslo pro Android (starší verze než Android 5.0 Lollipop, které nemají šifrování celého disku)
- Z dostupných informací plyne, že to v minulosti udělal pro DHS (vyšetřování dětské pornografie v Kalifornii), FBI (vyšetřování distribuční sítě kokainu v Novém Mexiku), Bureau of Land Management (vyšetřování pěstíren marihuany v Oregonu) a Secret Service (detaily nejsou známy)
- Operace vyžadovala využití existujících nástrojů ze strany Google/LEA

Význam FBI v. Apple – Going Dark

- Going Dark narativ od roku 2014
- Vystoupení na Brooking Institution, ředitel FBI James B. Comey:
  - FBI je konfrontována s vážnými hrozbami a k jejich potlačování potřebuje efektivní právní nástroje. V minulosti byl jedním z nástrojů soudní příkaz k odposlechu komunikace („data in motion“) a soudní příkaz umožňující přístup k zařízením („data at rest“).
  - Mnoho subjektů, které poskytují komunikační prostředky nepodléhá povinnostem umožnit odposlech. Dostupnost kryptografie pak může způsobit, že soudní příkaz může být nevykonatelným kusem papíru.
- Comey postoj zopakoval před Senate Select Committee on Intelligence a před Senate Judiciary Committee

Dva rozměry Going Dark

- Data in motion – FBI není schopna zajistit příkaz k odposlechu pro všechny služby, přes které probíhá komunikace
- Data at rest – šifrování způsobuje, že FBI není fakticky schopna vykonat soudní příkaz

- Řešení: vhodná legislativní změna rozšiřující okruh povinných subjektů pro data in motion a umožňující v odůvodněných situacích nahlédnout pod pokličku pro data at rest

FBI v. Apple v médiích

- Široká pozornost
- FBI dokázala, že má své limity a usnadnila si pozici pro lobbing
- Apple ukázal veřejnosti, jak fungují některé bezpečnostní prvky
  - Fire OS má šifrování teprve od loňského podzimu, ale nikoho to moc nezaujalo
- Demonstrace nových technologií na hmatatelném telefonu namísto abstraktních metadat

Nepanikařte – ručník si brát nemusíte

- Don‘t Panic. Making Progress on the „Going Dark“ Debate.
  - Berkman Center for Internet & Society při Harvardské univerzitě – Urs Gasser, Jack Goldsmith, Susan Landau, Bruce Schneier, Jonathan Zittrain a další.
- Závěry:
  - Je nepravděpodobné, že end-to-end šifrování přijmou všechny společnosti.
  - Možnost monitorovat zabezpečený kanál (data in motion, data at rest) může být snížena, pokud technologický vývoj nabídne alternativu (IoT)
  - Metadata nejsou šifrována a většina nikdy nebude – naučte se je používat.
  - Patrikulární diskuze musí být následována širší diskuzí nad proměnou individuálního soukromí a kolektivní bezpečnosti.

Jak jsme na tom v ČR?

- Zakázka „Dekódování šifrovaných datových komunikací“
  - Zřejmě směřuje k efektivní alokaci zdrojů
- Stanovisko ÚZČ:
  - postupem dle §158d TŘ je možné sbírat informace utajovaně. Aby mohly prostředky sloužit k utajovanému použití, je nutné utajovat jejich princip, funkci a provedení. Ve chvíli, kdy je PČR umožněno se s obsahem zákonně seznámit, musí mít okamžitě k dispozici nástroje. PČR tedy nepotřebuje zvláštní zákonné zmocnění k dešifrování komunikace, kterou je oprávněna zachytit (obdoba překladu z neznámého jazyka).

Dotazy?