



Výzkumná zpráva Kongresu

**Využití technologií pro boj s
kriminalitou**

FABIAN BLAŽEK



PRO ČESKÝ MODEL AMERICKÉHO KONGRESU 2020



1. Úvod

Moderní technologie otevírají bezpečnostním složkám, jako jsou policie, tajné služby (FBI) či protidrogová police (DAE), možnosti, o kterých se jim před několika lety ani nesnilo. Ať už se jedná o sledování podezřelého dronem, jeho lokaci přes GPS signál, vniknutí do účtů na sociálních sítích a sledování jeho konverzací nebo o jiné metody. Technologie s sebou přináší nové možnosti, díky kterým lze policejní vyšetřování výrazně urychlit, nebo dokonce předejít trestnému činu. Druhá strana mince je ovšem ztráta soukromí, která s použitím takových technologií hrozí. Vzpomeňme na četné skandály masového odposlouchávání americké tajné služby NSA. Takové technologie, jako je rozpoznávání obličejů či nabourání se do osobních účtů, představují riziko vzniku všemocného Orwellovského státu.

Tato zpráva podává stručný přehled o existujících zákonech, které svým rozsahem představují riziko vniknutí do soukromí amerického občana. Následně popisuje současný stav zákonů o technologiích, jako jsou monitorovací aktivity na internetu a potenciální využití dronů, prezentuje různé úhly pohledu a předkládá možná další legislativní opatření.

2. Historický kontext a stávající zákony

2.1 Ústava

Právo na soukromí hrálo v historii Spojených států vždy velkou roli. Hned čtvrtý dodatek americké Ústavy se k této otázce vyjadřuje a stanovuje zde na první pohled jasná pravidla: *„Právo národa na ochranu svobody osobní a domovní, písemností a majetku nesmí být porušováno neoprávněnými prohlídkami a konfiskacemi; nesmí být vydán rovněž žádný příkaz, který by se neopíral o zdůvodněná zjištění, doložená přísahou nebo jiným způsobem potvrzená, a který by neobsahoval přesné určení místa, které má být prohledáno, přesný popis osob, které mají být vzaty do vazby, a věcí, jež mají být zabaveny.“*¹ Ústava, napsaná v roce 1787, samozřejmě nemohla předvídat překotný vývoj technologií ve 20. a 21. století, jasně ovšem stanovuje mantinely, které nesmí být vládou překročeny, a mezi ně lze také zahrnout moderní technologie. Ústava zde jasně hovoří o pravidlech, která by měly bezpečnostní složky v případě sledování podezřelé osoby dodržovat. Povolení k narušení soukromí tedy musí být vždy podloženo (soudním) oprávněním a dobrým odůvodněním. Můžeme tedy víceméně konstatovat, že nedovolené sledování soukromých konverzací na sociálních sítích, ukládání informací získaných pomocí kamer s funkcí rozpoznání obličeje nebo sledování drony může být v některých případech protiústavní.

¹ Fourth Amendment | U.S. Constitution | US Law | LII / Legal Information Institute. LII / Legal Information Institute [online]. Dostupné z: https://www.law.cornell.edu/constitution/fourth_amendment



2.2 FISA (Foreign Intelligence Surveillance Act, 1978)²

Tento zákon vstoupil v platnost za vlády prezidenta Cartera a od té doby byl několikrát novelizován. Cílem zákona je umožnit bezpečnostním složkám efektivnější boj proti terorismu přicházejícímu ze zahraničí. Boj proti potenciálním teroristům se však vztahuje i na domácí půdu. Zákon se snaží stanovit jasná pravidla pro zásah do osobních svobod (např. sledování elektronické komunikace, mobilní odposlechy atd.) bezpečnostními složkami a zároveň se jim snaží poskytnout takové pravomoce, aby svoji práci mohly vykonávat efektivně a rychle. Jeho nejznámější úprava byla provedena schválením známého *The Patriot Act*, kterým se bude zpráva zabývat níže samostatně.³

2.3 ECPA (Electronic Communications Privacy Act, 1986)⁴

Tento zákon stanovuje podmínky, které musí bezpečnostní složky splnit, aby mohly sledovat mobilní a především internetovou komunikaci amerických občanů v případech podezření. Týká se komunikace přes mobilní zařízení, dále přes email a data uložená elektronicky. Stanovil různé druhy soudních povolení k získání informací a také podmínky o případné nutnosti informovat podezřelé osoby o sledování. Nařizuje zákaz používání nelegálně (tedy bez soudního povolení) získaných elektronických informací jako důkazů při soudním řízení.⁵ Dále chrání data uživatelů, která jsou uložena u poskytovatelů služeb (mobilní operátoři atd.) Zákon byl několikrát doplněn a novelizován, aby odpovídal aktuálnímu vývoji technologií.

2.4 The USA Patriot Act (2001)⁶

The USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) byl schválen krátce po teroristických útocích dne 11. září 2001 a navazoval na výše zmíněné zákony. Jeho cílem bylo předejít teroristickým útokům na americké půdě přicházejícím jak z domova, tak ze zahraničí. *The Patriot Act* poskytl zatím největší prostředky bezpečnostním složkám v boji proti terorismu. Vláda mohla nově sledovat a odposlouchávat americké občany podezřelé z terorismu téměř bez soudního povolení (tzv. bulk wiretap)⁷ a v některých případech mohla získat přístup k platebním kartám a osobním informacím na internetu. Zákon také umožnil agenturám, jako je NSA,

² The Foreign Intelligence Surveillance Act of 1978. Justice Information Sharing [online]. Dostupné z: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286>

³ [online]. Dostupné z: https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf

⁴ Electronic Communications Privacy Act of 1986. Justice Information Sharing [online]. Dostupné z: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>

⁵ 18 U.S. Code § 2515 - Prohibition of use as evidence of intercepted wire or oral communications | U.S. Code | US Law | LII / Legal Information Institute. LII / Legal Information Institute [online]. Dostupné z: <https://www.law.cornell.edu/uscode/text/18/2515>

⁶ EPIC - USA PATRIOT Act (H.R. 3162). EPIC - Electronic Privacy Information Center [online]. Copyright © 1994 [cit. 15.04.2020]. Dostupné z: <https://epic.org/privacy/terrorism/hr3162.html>

⁷ Dříve v zásadě platilo pravidlo, že se soudní povolení vztahuje na konkrétní mobilní zařízení. Tato nová pravomoc umožňuje sledování podezřelého i v případě, že si opatří nový mobil.



masový sběr telefonních a internetových dat.⁸ Zákon se stal rychle kontroverzním, ovšem v kontextu 11. září byl vnímán spíše jako rozumné opatření. Tehdejší šéf FBI Robert Mueller při slyšení před soudní komisí v roce 2004 řekl, že *The Patriot Act* pomohl velmi výrazně FBI v boji proti terorismu a že bez tohoto zákona by její práce byla značně omezená.⁹ Zákon byl za svojí existence několikrát novelizován a v roce 2015, za vlády Baracka Obamy, nahrazen upraveným *The Freedom Act*.¹⁰ Dodnes je některými právníky, senátory a neziskovými organizacemi velmi kritizován za to, že umožňoval ve jménu národní bezpečnosti vládě beztestně narušovat soukromí amerických občanů.

2.5 The Freedom Act (2015)

The Freedom Act upravoval a navazoval na *The Patriot Act*, který se stal po aféře s Edwardem Snowdenem znovu velmi kontroverzním. Proto *The Freedom Act* stanovil přísnější podmínky pro získávání informací bezpečnostními složkami, aby bylo více chráněno soukromí jednotlivce, a zároveň se snažil zachovat dostatečné množství pravomocí pro efektivní boj proti zahraničnímu i vnitrostátnímu terorismu. Hlavní změna oproti *The Patriot Act* se týkala zákazu masového shromažďování telefonních dat (umožněného podle odstavce 215 v *The Patriot Act*).¹¹ Podle kritiků ale omezení nejsou dostatečná a stále dávají bezpečnostním složkám přehnané pravomoci k zasahování do soukromí Američanů.¹²

2.6 Aféra s Edwardem Snowdenem

Zásadní obrat ve veřejném mínění, které bylo větším pravomocem ze strany bezpečnostních složek po 11. září spíše nakloněno, přišel po aféře s bývalým zaměstnancem CIA Edwardem Snowdenem. Ten poskytl údajně přísně utajené informace deníkům *The Washington Post* a *The Guardian*,^{13 14} zveřejnění těchto informací následně vyvolalo celosvětový skandál.

⁸ Fact Sheet: Section 215 of the USA PATRIOT Act | Center for Strategic and International Studies. Center for Strategic and International Studies | [online]. Copyright © 2014 by the Center for Strategic and International Studies. All rights reserved. [cit. 15.04.2020]. Dostupné z: <https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act>

⁹ Patriot Act - HISTORY. [online]. Copyright © 2020 A [cit. 15.04.2020]. Dostupné z: <https://www.history.com/topics/21st-century/patriot-act>

¹⁰ H.R.3162 - 107th Congress (2001-2002): Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 | Congress.gov | Library of Congress. Congress.gov | Library of Congress [online]. Dostupné z: <https://www.congress.gov/bill/107th-congress/house-bill/03162>

¹¹ FACT SHEET: Implementation of the USA FREEDOM Act of 2015. Home [online]. Dostupné z: <https://www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015>

¹² Surveillance Under the Patriot Act | American Civil Liberties Union. American Civil Liberties Union [online]. Dostupné z: <https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>

¹³ NSA Prism program taps in to user data of Apple, Google and others | US news | The Guardian. [online]. Copyright © 2020 Guardian News [cit. 15.04.2020]. Dostupné z: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>





Jednalo se o uniklou prezentaci o postupu americké tajné služby NSA, která se měla dopouštět masivního sběru dat ve spolupráci s internetovými giganty. Tajný program s názvem „PRISM” měl mít ve spolupráci s většinou amerických internetových firem skoro neomezený přístup k jejich serverům s uloženými informacemi o uživateli (ve formě emailů, chatů, fotografií atd.). Firmy k tomu údajně měly dát dobrovolný souhlas. Ovšem ty v reakci na aféru jakoukoliv spolupráci s bezpečnostní agenturou NSA popřely a tvrdily, že o ničem takovém nevěděly. Program měl shromažďovat a ukládat informace o velkém počtu lidí nejspíš za účelem vytvoření databáze pro boji proti terorismu. To všechno se mělo dít bez vědomí poskytovatelů dat, uživatelů a především bez vědomí soudů, které k podobné aktivitě musí vydat oprávnění. V reakci na to se vytvořil společenský tlak na zákonodárce, aby bezpečnostní složky v této oblasti nějak limitovali. Snowden před zveřejněním informací uprchl do Hongkongu a následně do Ruska. Nicméně jeho informace nebyly potvrzeny a většina zmíněných firem či agentur takové nařčení odmítá. Tehdejší šéf FBI James Clapper přiznal existenci programu PRISM, uvedl ale, že se jedná o program, který shromažďuje důležité informace pouze na základě soudního povolení. Uvedl také dva příklady, kdy se díky programu podařilo předejít teroristickým útokům – na newyorské metro a na redakci dánských novin.¹⁵

2.7 Využití mobilních telefonů a internetového obsahu při boji s kriminalitou

Jednou z hojně využívaných oblastí pro zdroj informací při boji s kriminalitou jsou mobilní telefony, internetová komunikace a celkově osobní informace na internetu, které jsou uloženy v databázích. V mobilních telefonech se o podezřelém může ukrývat ohromné množství dat, která jsou často klíčová při policejním vyšetřování. S příchodem chytrých telefonů a sociálních sítí se situace pro případné kriminálníky o to víc ztížila, jelikož většina poskytovatelů těchto služeb (např. Google, Microsoft, Facebook atd.) si ukládá informace o svých uživateli na vlastní servery, což v praxi vytváří obrovskou databázi informací, která se může při vyšetřování náramně hodit. Přestože služby, jako je WhatsApp, používají šifrovaný přenos zpráv a na svých stránkách zdůrazňují, že poskytnou informace bezpečnostním složkám pouze v případě soudního příkazu,¹⁶ je nasnadě se domnívat, že se ne vždy tak děje. Americká legislativa se vůči nedovolenému vniknutí bezpečnostních složek do soukromí občanů může zdát poměrně přísná, nicméně realita je často někde jinde. Obecně platí pravidlo, že se policie či tajná služba v současné době může legálně dostat k datům v mobilu či na internetu pouze přes nějakou formu soudního povolení.¹⁷ Příslušný

¹⁴ Washingtonpost.com [online]. Dostupné z: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

¹⁵ Aktuálně - Aktuálně.cz [online]. Copyright © [cit. 15.04.2020]. Dostupné z: <https://www.aktualne.cz/wiki/zahranici/prism/r~i:wiki:3799/>

¹⁶ Whatsapp.com [online]. Dostupné z: <https://faq.whatsapp.com/en/general/26000050>

¹⁷ When is law enforcement allowed to search your phone? - Vox. Vox - Understand the News [online]. Copyright © 2020 [cit. 15.04.2020]. Dostupné z: <https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-password-rights>





soud tedy musí vydat povolení k určitým krokům v rámci vyšetřování. Jedná se buď o získání informací od třetích stran – těmi jsou míněny hlavně firmy jako Google, Facebook a Microsoft, při jejichž používání uživatel souhlasí s ukládáním dat a které mají povinnost na základě soudního nařízení informace o podezřelém vydat – nebo se můžou bezpečnostní složky se soudním povolením dokonce nabourat do chytrých telefonů, či dokonce přemluvit ke spolupráci někoho, kdo s vámi vede internetovou konverzaci.¹⁸ K odposlechu hovorů je rovněž nutné soudní povolení. V některých případech ovšem bezpečnostní složky mohou použít i zařízení, které sleduje čísla volajících, a to i bez povolení,¹⁹ stejně je tomu i v případě sledování polohy či zjištění IP adresy podezřelého.²⁰ Samotné získání soudního příkazu ovšem může trvat dlouho, a může tak brzdit rychlost vyšetřování. Z toho, co víme o tajných sledovacích programech, jako je PRISM, můžeme vidět, že si bezpečnostní složky jsou schopny najít zadní vrátka, jak se k informacím ze zařízení dostat.²¹

2.8 Prostor pro zákony

Otázkou tedy je, jestli je důležitější soukromí, nebo efektivita a rychlost policejního vyšetřování. Proto je zde prostor pro legislativu, která by například upravila pravidla získávání informací o amerických občanech od třetích stran. A to buď jinak než skrze soudní povolení, nebo by dokonce zakazovala bezpečnostním složkám spolupráci s třetími stranami, které o občanech mohou mít uložená data. Další možností může být povinnost uvědomění podezřelého o sledování jeho internetové komunikace nebo zákaz shromažďování velkého množství dat pod záminkou vytvoření databáze o rizikových uživatelích.

2.9 Použití dronů policií při boji s kriminalitou

Čím dál více používanou technologií se v poslední době stávají tzv. UAVs (*unmanned aerial vehicles*) neboli drony. Americká armáda je již zařadila mezi běžnou výbavu, a to především pro jejich přesnost, absenci pilota přímo ve stroji a relativní nenápadnost. Jejich přesnost a spolehlivost se ukázala například při zabití íránského generála Sulejmáního. Možnost využití v tomto případě nevojenských dronů se otevírá i na území Spojených států. Drony se nabízejí jako nová a efektivní technologie při boji s kriminalitou, a to hned z několika důvodů. Jednak jsou to finanční náklady, které jsou v porovnání s provozem policejního vrtulníku mnohem nižší. Drony jsou rovněž schopny monitorovat obrovskou plochu v poměrně krátkém čase, což může velmi pomoci při vyšetřování, kdy je potřeba získat informace rychle.

¹⁸ When is law enforcement allowed to search your phone? Vox - Understand the News [online]. Copyright © 2020 [cit. 15.04.2020]. Dostupné z: <https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-password-rights>

¹⁹ Can Police Tap Your Phone Without Your Knowledge?. JacksonWhite Attorneys at Law | Mesa & Phoenix, Arizona [online]. Copyright © JacksonWhite PC, 2019, All Rights Reserved [cit. 15.04.2020]. Dostupné z: <https://www.jacksonwhitelaw.com/criminal-defense-law/legal-police-tap-phone/>

²⁰ Can Police Tap Your Phone Without Your Knowledge?. JacksonWhite Attorneys at Law | Mesa & Phoenix, Arizona [online]. Copyright © JacksonWhite PC, 2019, All Rights Reserved [cit. 15.04.2020]. Dostupné z: <https://www.jacksonwhitelaw.com/criminal-defense-law/legal-police-tap-phone/>

²¹ PRISM - Aktuálně.cz. Aktuálně - Aktuálně.cz [online]. Copyright © [cit. 15.04.2020]. Dostupné z: <https://www.aktualne.cz/wiki/zahranici/prism/r~i:wiki:3799/>





Také jejich hlučnost je mnohem nižší, a proto se hodí na nepozorované sledování podezřelého. Personál je v případě použití dronu mimo nebezpečí a ovládání je také jednodušší, proto se ho může naučit téměř každý. Pokud by byly v budoucnu používány verze disponující zbraněmi, lze je také využít v rizikových situacích, při nichž by člen ozbrojených složek mohl být vystaven vážnému nebezpečí. Dále je třeba zmínit možnost využívání termokamer. Na druhou stranu jsou zde také značná rizika používání dronů bezpečnostními složkami. Především se jedná o hrozbu narušení soukromí a nedovolené sledování. S překotným vývojem technologií by mohlo dojít k tomu, že drony budou schopny odposlechu či právě používání termokamer, což by mohlo být vážné ohrožení soukromí jednotlivce. Velké riziko je také automatizace dronů, kdy může sledování probíhat na principu autopilota. Další novou výzvou pro soukromí občanů jsou drony opatřené kamerami na rozpoznávání obličeje a státních poznávacích značek. Bezpečnostní složky by si tak mohly vytvořit obsáhlou databázi a mít neustálý dohled nad velkým počtem lidí. Pokud tedy federální vláda nenastaví v této oblasti jasné hranice, může docházet k porušování čtvrtého dodatku *Ústavy*.

Zákony, které nějakým způsobem limitují používání dronů bezpečnostními složkami, jsou zatím v platnosti pouze v jednotlivých státech. V některých z nich musí policie získat soudní povolení k použití dronu (jsou to např. Florida, Maine, Virginia a Severní Dakota), ovšem situaci lze obejít použitím sofistikovanějšího sledování z letadla.²²

Na federální úrovni lze vycházet z pravidel, která stanovila FAA (*Federal Aviation Agency*). Ta zařadila v roce 2015 drony do národního vzdušného prostoru a v roce 2020 stanovila pravidla, podle nichž majitelé dronů musí získat certifikované sledovací číslo a projít krátkým školením přímo od FAA.²³ Co se týče potenciálního sledování drony, dá se částečně vycházet ze dvou rozhodnutí Nejvyššího soudu. První z nich, *Florida v. Riley*,²⁴ se týkal případu, kdy policie přeletěla vrtulníkem nad zahradou údajného pěstitele marihuany, aby mohla získat usvědčující důkazy. Pan Riley nařkl policii z narušení soukromí a celý případ se dostal až k Nejvyššímu soudu. Ten rozhodl ve prospěch policie s odůvodněním, že přelet vrtulníkem ve výši přes 400 stop (cca 120 metrů) je ve veřejném vzdušném prostoru, a proto nezasahuje do vlastnictví pozemku občana. Přelet by tedy legálně mohl provést kdokoli s osobním letadlem. Podobně jako je možný výhled na pozemek ze silnice či jiné cesty, není potřeba získat soudní povolení k vykonání přeletu za účelem získání informací, které jsou volně viditelné. Dále v rozsudku stojí, že jednání nebylo protizákonné, jelikož na jeho základě policie nezjistila žádné příliš osobní detaily o jedinci. Podezření policie na pěstování

²² Drones and aerial surveillance: Considerations for legislatures. Brookings - Quality. Independence. Impact. [online]. Dostupné z: <https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/>

²³ <https://www.faa.gov/uas/>

²⁴ *Florida v. Riley* :: 488 U.S. 445 (1989) :: Justia US Supreme Court Center. Justia US Supreme Court Center [online]. Copyright © 2020 [cit. 15.04.2020]. Dostupné z: <https://supreme.justia.com/cases/federal/us/488/445/>





marihuany se (pro zajímavost) potvrdilo. V případě *Dow Chemical Co. v. United States*²⁵ se chemická firma Dow soudila s agenturou na ochranu životního prostředí (EPA) za to, že nedovoleně podnikla sledovací akci jejich továrny po tom, co jim firma nedovolila inspekci. Soud zde, stejně jako v minulém případě, rozhodl ve prospěch žalovaného. Tedy že použití kamery na mapování průmyslového komplexu z veřejného vzdušného prostoru není v rozporu se čtvrtým dodatkem *Ústavy*.²⁶

3. Prostor pro novou legislativu

Je tedy nasnadě předložit takovou legislativu, která bude reagovat na rychlý vývoj technologií a jím způsobená rizika masového (i automatizovaného) sledování, rozpoznávání obličejů a poznávacích značek. Zároveň ale vezme v potaz výhody, které použití dronů při boji se zločinem nabízí (např. již zmíněné nízké náklady, rychlost, efektivita a bezpečí členů bezpečnostních složek). Legislativa může jít cestou soudního povolení, které by bylo potřebné k použití sledování podezřelé osoby. Může také stanovit pravidla pro takové sledování (pouze na omezený čas atd.), zakázat ukládání videozáznamu do databází nebo zakázat používání kamer s rozpoznáním obličeje.

4. Závěr

Můžeme vidět, že technologie nabízejí obrovský potenciál pro boj s kriminalitou a že se jejich schopnosti budou neustále zdokonalovat. Je tedy nasnadě vzít v potaz všechny pro a proti moderních technologií a vytvořit na federální úrovni takovou legislativu, která poskytne bezpečnostním složkám efektivní prostředky na boj proti kriminalitě a zároveň bude chránit soukromí amerických občanů před možným zneužitím.

²⁵ *Dow Chemical Co. v. United States* :: 476 U.S. 227 (1986) :: Justia US Supreme Court Center. Justia US Supreme Court Center [online]. Copyright © 2020 [cit. 15.04.2020]. Dostupné z: <https://supreme.justia.com/cases/federal/us/476/227/>

²⁶ *Brookings. Brookings - Quality. Independence. Impact.* [online]. Dostupné z: <https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/>





5. Zdroje

House Committee on Homeland Security. *Home* / *House Committee on Homeland Security* [online]. Dostupné z: <https://homeland.house.gov/preparing-for-the-future-an-assessment-of-emerging-cyber-threats>

FACT SHEET: Implementation of the USA FREEDOM Act of 2015. *Home* [online]. Dostupné z: <https://www.intelligence.gov/index.php/ic-on-the-record-database/results/787-fact-sheet-implementation-of-the-usa-freedom-act-of-2015>

Brookings. *Brookings - Quality. Independence. Impact.* [online]. Dostupné z: <https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures/>

Surveillance Under the Patriot Act | American Civil Liberties Union. *American Civil Liberties Union* [online]. Dostupné z: <https://www.aclu.org/issues/national-security/privacy-and-surveillance/surveillance-under-patriot-act>

<https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285> Electronic Communications Privacy Act of 1986. *Justice Information Sharing* [online]. Dostupné z: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>

[online]. Dostupné z: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

NSA Prism program taps in to user data of Apple, Google and others | US news | The Guardian. [online]. Copyright © 2020 Guardian News [cit. 15.04.2020]. Dostupné z: <https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>

Can Police Tap Your Phone Without Your Knowledge?. *JacksonWhite Attorneys at Law | Mesa & Phoenix, Arizona* [online]. Copyright © JacksonWhite PC, 2019, All Rights Reserved [cit. 15.04.2020]. Dostupné z: <https://www.jacksonwhitelaw.com/criminal-defense-law/legal-police-tap-phone/>

When is law enforcement allowed to search your phone? - Vox. *Vox - Understand the News* [online]. Copyright © 2020 [cit. 15.04.2020]. Dostupné z: <https://www.vox.com/recode/2020/2/24/21133600/police-fbi-phone-password-rights>

Patriot Act - HISTORY. [online]. Copyright © 2020 A [cit. 15.04.2020]. Dostupné z: <https://www.history.com/topics/21st-century/patriot-act>

PRISM - Aktuálně.cz. Aktuálně - Aktuálně.cz [online]. Copyright © [cit. 15.04.2020]. Dostupné z: <https://www.aktualne.cz/wiki/zahranici/prism/r~i:wiki:3799/>





[online]. Dostupné

z: https://www.fletc.gov/sites/default/files/imported_files/training/programs/legal-division/downloads-articles-and-faqs/research-by-subject/miscellaneous/ForeignIntelligenceSurveillanceAct.pdf

Whatsapp.com [online]. Dostupné z: <https://faq.whatsapp.com/en/general/26000050>

Fact Sheet: Section 215 of the USA PATRIOT Act | Center for Strategic and International Studies. Center for Strategic and International Studies | [online]. Copyright © 2014 by the Center for Strategic and International Studies. All rights reserved. [cit. 15.04.2020]. Dostupné z: <https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act>

Fourth Amendment | U.S. Constitution | US Law | LII / Legal Information Institute. LII / Legal Information Institute [online]. Dostupné z: https://www.law.cornell.edu/constitution/fourth_amendment

The Foreign Intelligence Surveillance Act of 1978. *Justice Information Sharing* [online]. Dostupné z: <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1286>

EPIC - USA PATRIOT Act (H.R. 3162). *EPIC - Electronic Privacy Information Center* [online]. Copyright © 1994 [cit. 15.04.2020]. Dostupné z: <https://epic.org/privacy/terrorism/hr3162.html>



