# Apple vs. FBI: etická dimenze kryptografie

**Radek Návrat**

**Anotace**

*Následující text se zabývá etickou rovinou silného šifrování. Ta je přiblížena prostřednictvím popisu a analýzy sporu, jenž se v roce 2016 odehrál mezi společností Apple a FBI. V rámci explanace této kauzy je konceptualizován utilitaristický a deontologický přístup, jež se zde střetly, přičemž vůči deontologii je předložen protiargument vycházející z teorie kulturního lagu. Kromě tohoto se ale text zaměřuje i na popis historické paralely sporu, jež také může posloužit při jeho posuzování.*

**Summary**

*The following text is aimed at the ethical dimension of strong cryptography. It is outlined through description and analysis of dispute which was taking place between Apple and FBI in 2016. In explaining this case is conceptualized utilitaristic and deontological approach that conflicted with each other. Against deontology is presented counter-argument coming from the theory of cultural lag. In addition to that, the study is also focused on the description of a historical parallel of the dispute which may be used for its evaluation.*

**Klíčová slova:** Apple, deontologie, etika, FBI, kryptografie, šifrování, terorismus, utilitarismus

**Keywords:** Apple, deontology, ethics, FBI, cryptography, encryption, terrorism, utilitarianism

Historie kryptografie se až do sedmdesátých (resp. čtyřicátých) let minulého století nesla v duchu názoru Edgara Allana Poea, který tvrdil, že nemůže být sestrojena taková šifra, pro kterou by lidský intelekt nebyl hrozbou[1]. Příchod technologie výpočetního stroje a jím zprostředkovaných technik, jakými jsou například asymetrické *šifrování* či Diffieho-Hellmanova výměna *klíčů*, však umožnily informace zabezpečit způsobem, který dokáže vzdorovat nejen intelektu jednoho člověka, ale i snahám o prolomení, které iniciují takové entity jako je stát[2].

Tato — řekněme — paradigmatická změna, kterou navíc umocnilo masivní rozšíření ICT (Informační a komunikační technologie) na bázi mikroprocesoru, však s sebou přinesla morální dilemata, jež se v zásadě dotýkají buďto možnosti nějaké informace takto silně zabezpečit, nebo to naopak odepřít či podrýt.[3] „Horror“, kde se spolu tyto dvě pozice střetly, pak nastal relativně nedávno. Na začátku roku 2016 se totiž do pře dostaly společnosti Apple a FBI, přičemž jablkem jejich sváru bylo umožnění přístupu k informacím v šifrovaném iPhonu, který používal terorista, jenž v USA zosnoval největší útok od 11. září 2001.

**ISIS iPhone**

Druhého prosince roku 2015 na vánoční večírek v kalifornském San Bernardino zaútočil Sayed Rizwan Farook s manželkou Tashfeen. Při tomto útoku s islamistickým pozadím[4] zahynulo celkem 14 lidí a 22 jich bylo zraněno. Domovní prohlídka, následující po zneškodnění obou útočníků, pak odhalila, že Farook držel množství munice a materiál na výrobu bomb. V únoru 2016 se pozornost vyšetřovatelů tohoto teroristického útoku zaměřila na Farookův iPhone 5c, jehož zabezpečení však nedokázali prolomit a o asistenci tedy požádali výrobce — Apple Inc[5]. Ten to však striktně odmítnul, přičemž takto vytvořil silně rezonující kauzu, která „rozdělila Ameriku“[6]. Pro osvětlení pohnutek, které Apple vedly ke zdánlivě zarážejícímu nesouhlasu s požadavkem FBI, jež navíc posvětil i vlastník dotyčného telefonu (ten byl služební)[7], je však třeba říci, co vlastně bylo ze strany federálních vyšetřovatelů požadováno.

---

[1] Srov. Ingram, John, H. *Edgar Allan Poe: His Life, Letters, and Opinions*. Londýn: W. H. Allen And Co., 1886.

[2] Narayanan, Arvind. What Happened to the Crypto Dream?, Part 1. *IEEE.org* [on-line] 2013. [cit. 10. 3.2019]. Dostupné z: <http://ieeexplore.ieee.org/document/6493328/>.

[3] Tavani, Herman. The Conceptual And Moral Landscape of Computer Security. In *Internet Security: Hacking, Counterhacking, and Society*. Himma, Kenneth Einar (ed.). Londýn: Jones and Bartlett, 2007.

[4] Borger, Julian. San Bernardino shooters radicalized as early as 2013, says FBI head. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/us-news/2015/dec/09/no-evidence-san-bernardino-attackers-part-of-wider-cell-loretta-lynch>.

[5] Yardon, Danny et al. Inside the FBI's encryption battle with Apple. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>.

[6] CBS NEWS. CBS News poll: Americans split on unlocking San Bernardino shooter's iPhone. *CBS News* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone/>.

[7] Yardon, Danny et al. Inside the FBI's encryption battle with Apple. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>.

Telefony iPhone s operačním systémem iOS 8 a výše jsou kompletně šifrovány pomocí 256bitového neextrahovatelného klíče, který je v každém zařízení unikátní. K tomu, aby se uložené informace staly pro člověka čitelnými (aby došlo k dešifrování) je třeba ručně zadat šestimístný vstupní kód, který však může být chybně zadán jen třikrát za hodinu. Navíc je zde pak přítomna i funkce auto-erase, která — pokud je aktivní — po deseti chybných zadáních vstupního kódu dešifrovací klíč smaže. Situace, v níž se tedy FBI ocitla, byla zhruba taková, že nejsnadnější způsob získání informací z Farookova telefonu spočíval v postupném mechanickém zadávání všech hodnot v rozmezí 0 až 999 999, přičemž špatné zadání mohlo být učiněno pouze třikrát za hodinu (za předpokladu, že auto-erase nebylo aktivováno). Z tohoto důvodu tedy Apple požádala, aby jí vytvořil nový operační systém, který by mohl být spuštěn v RAM telefonu a který by umožňoval vstupní kód zadávat skrze port (tzn. pomocí programu na jiném počítači) bez omezení „třikrát za hodinu“ a bez možnosti aktivování funkce auto-erase. A požadavek na výrobu tohoto nového operačního systému — tohoto univerzálního klíče ke všem mobilním zařízením své provenience — byl tím, co Apple odmítl.

Celá věc krátce po vyjádření negativního postoje Applu zamířila k soudu, který v rámci nejnižší instance požadavek FBI posvětil příkazem[8], který argumentoval zákonem *All Writs Act*[9] (1789, resp. 1911). Apple se však odvolal a celá věc se během měsíce měla posunout před federální soud ve Washingtonu. K tomuto stání ale nikdy nedošlo, jelikož FBI den před ním požádala o dvoutýdenní odklad z důvodu, že „*třetí strana demonstrovala možnou metodu odemčení telefonu*“.[10] Týden na to pak federální vyšetřovatelé svou žádost o soudní příkaz zcela stáhli, protože se jim „*data uložená ve Farookově telefonu podařilo plně zpřístupnit*“[11], což deník Washington Post připsal „*pomoci profesionálních hackerů*“[12], kteří využili chybu nultého dne. Po jednání senátní komise pro zpravodajské služby, které se uskutečnilo počátkem května roku 2017 pak toto potvrdila i senátorka Feinsteinová, která navíc prozradila, že FBI za tuto službu zaplatila celkem 900 000 dolarů.[13]

[8] Pym, Sheri. ORDER COMPELLING APPLE, INC. TO ASSIST AGENTS IN SEARCH. [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.documentcloud.org/documents/2714001-SB-Shooter-Order-Compelling-Apple-Asst-iPhone.html>.

[9] Viz US LEGAL. *All Writs Act Law and Legal Definition*. [on-line] nedat. [cit. 5. 3.2019]. Dostupné z: <https://definitions.uslegal.com/a/all-writs-act%20/>.

[10] Wilkinson, Tracy, L. *MEMORANDUM OF POINTS AND AUTHORITIES*. [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.documentcloud.org/documents/2773542-031123152171.html#document/p3>.

[11] Wilkinson, Tracy, L. *GOVERMENT'S STATUS REPORT*. [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.scribd.com/doc/306202728/FBI-apple-20160328#from_embed>.

[12] Nakashima, Ellen. FBI paid professional hackers one-time fee to crack San Bernardino iPhone. *Washington Post* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.b09b1af01648>.

[13] AP. Senator reveals that the FBI paid $900,000 to hack into San Bernardino killer's iPhone. *CNBC* [on-line] 2017 [cit. 5. 3.2019]. Dostupné z: <https://www.cnbc.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html>.

Nehledě na to, jak celá věc dopadla (nebo nedopadla) obrysy toho, co se událo zůstaly nicméně na stole a s nimi i scénář, který si — vzhledem k tomu, že může kdykoliv nastat znovu — žádá mravní soud.

> *K dispozici je výpočetní zařízení, které bylo před tím využíváno teroristou. Toto zařízení může obsahovat informace které pomohou jeho vyšetřování nebo dokonce záchraně lidských životů. Jediným způsobem, jak se k informacím v tomto zařízení dostat je však vytvoření „speciálního klíče", který bude moci být použit ke zpřístupnění jakéhokoliv jiného zařízení. Je správné, aby byl za těchto podmínek dotyčný klíč vytvořen a použit?*

**O etice a bezpečnosti**

Nehledě na to, že pře mezi Applem a FBI byla v rámci své oficiální roviny především soudním sporem, což bylo takto podáváno i médii, její centrální aktéři reprezentovaní výkonným ředitelem Applu Timem Cookem a ředitelem FBI Jamesem Comeym, k celé věci přistupovali z pozice normativní etiky. V jejich vyjádřeních[14], která se objevila záhy po prvním soudním státní, tak byly předloženy argumenty, které na straně FBI vycházely z deontologie a na straně Applu zase z konsekvencialismu (resp. utilitarismu). To, co proti sobě v této ostře sledované debatě stanulo, tedy bylo, obecně řečeno, buďto umožnění specifického způsobu vyšetřování, který je správný, protože je vedený povinností a počestnými pohnutkami, nebo naopak jeho tabuizace, která je správná, protože tento způsob přinese více škody než užitku (následky existence „superklíče"). K tomuto je pak ještě nutno doplnit, že oba aktéři sporu v této při operovali i s přisouzením břemene principal-agent[15]. FBI by totiž naplněním svého požadavku získala „superklíč" nebo precedent a Apple by takto zase zamezil nepochybnému poškození dobrého jména svého produktu, a navíc by takto mohl vydělat i v oblasti PR.

Mimo rozdílu spočívajícího v rozporném názoru na schéma usuzování, jež má být základem reakce v dané situaci, je však tento spor signifikantní i tím, že jde o střet dvou rozdílných koncepcí bezpečnosti. Nehledě na jisté momenty[16] argumentace obou zainteresovaných stran či na to, jak tuto při mohly interpretovat určité skupiny lidí[17], předmětem sporu mezi Applem a FBI nebylo soukromí. Byla jím bezpečnost, a to bezpečnost dosažená buďto regulací silného šifrování, nebo naopak jeho nedotknutelností.

---

[14] Viz Comey, James. We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead. *Lawfare* [on-line] 2016 [cit. 5. 3.2018]. Dostupné na: <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>. Cook, Tim. A Message to Our Customers. *Apple* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.apple.com/customer-letter/>.

[15] Ibidem.

[16] Ibidem.

[17] Viz např. cdn.cultofmac.com

*Bude bezpečněji, pokud před výkonem policejní autority nebude existovat neproniknutelné digitální útočiště, nebo bude bezpečněji, když toto útočiště existovat bude, nebude existovat žádný způsob k jeho narušení a toto útočiště bude sloužit i k ochraně před zločinem?*

**Meze deontologie – Ogburnův argument**

Mimo výše uvedeného dilematu, které spadá do rámce bezpečnosti počítačové etiky formulované Kennethem Himmou[18], jde však o konstrukci normativních soudů, s nimiž přišli Apple a FBI, smýšlet i jako o modelových příkladech pro posuzování ICT v dimenzi, kterou do etiky vnesli třeba Eugene Spafford[19] nebo Paul Thompson[20]. Spafford totiž například ve svém odsouzení implikací hackerského étosu v otázce narušování systémů přišel s jeho deontologickou kritikou, kterou postavil na oddělení činů a jejich důsledků, jež podle něj — pokud chtějí zůstat morálními — nemají překračovat hodnotu soukromí, přičemž jedinou opodstatnitelnou výjimkou je pouze národní bezpečnost. Thompson se pak na rozdíl od Spafforda v této otázce přiklonil k utilitarismu, a to s argumentem, že soukromí je vlastně jakýmsi derivátem obecné bezpečnosti a z důvodu této jeho amorfnosti tedy bude lepší věnovat pozornost právě této obecné bezpečnosti, a to prostřednictvím metod risk assessmentu.

I přesto, že se Spafford a Thompson ve svých tezích zabývali především otázkou vzešlou z problematiky soukromí (kterou Thompson označil jako podružnou), jejich pozice jdou vztáhnout i ke sporu mezi Applem a FBI, a to mimo jiné proto, že rámec Thompsonovy (resp. Gotliebovy[21]) námitky vůči soukromí je dobře aplikovatelný i v tomto případě (stejně jako v mnoha jiných případech deontologických normativních soudů). Co je to totiž ona národní bezpečnost, kterou se zaštiťoval Spafford i FBI[22]? Je to schopnost zabránit akci teroristů? Nebo to je i schopnost zamezit ekonomickým škodám, případně schopnost zabezpečit komunikace klíčových představitelů státu? A právě takováto obtížnost (nebo dokonce nemožnost) zřetelné konceptualizace povinnosti je něco, čím je postižena i deontologická pozice FBI ve Farookově případu, což navíc poměrně jasně vyplývá i z výsledků studie[23], již několik měsíců před celým incidentem publikovalo pracoviště CSAIL při MIT. Její autoři zde totiž relativně důrazně podotýkají, že ten, kdo bude držitelem „superklíče“ k určitým ICT se sám

[18] Himma, Kenneth Einar. Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking. In *The Handbook of Information and Computer Ethics.* Himma, Kenneth Einar (ed.). Londýn: Jones and Bartlett, 2007, s. 191–219.

[19] Spafford, Eugene, F. Are Computer Hacker Break-ins Ethical? In *Internet Security: Hacking, Counterhacking, and Society*. Himma, Kenneth Einar (ed.). Londýn: Jones and Bartlett, 2007, s. 49–61.

[20] Thompson, Paul, B. Privacy, Secrecy and Security. *Ethics and Information technology*, roč. 3, č. 1, 2001.

[21] Gotlieb, Calvin, C. Privacy: A Concept Whose Time Has Come and Gone. In *Computers, Surveillance, and Privacy*. Lyon, David – Zureik, Elia (eds.). Minneapolis: University of Minnesota Press, 1997, s. 156–175.

[22] Comey, James, B. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?. *FBI.gov* [on-line] 2014 [cit. 5. 3.2019]. Dostupné z: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

[23] Abelson, Harold et al. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. [on-line] 2015 [cit. 5. 3.2019]. Dostupné z: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>.

obratem stane terčem mnoha snah o narušení vlastní bezpečnosti, jehož cílem bude takovýto nástroj získat (o tom může svědčit například incident se skupinou TSB[24]). Mimo toho však podle nich hrozí i ekonomické a mezinárodně–politické dopady, které nebudou nepodstatné. Kdo by si totiž chtěl kupovat produkt, o němž by věděl, že jeho zabezpečení může být kompromitováno? A co by měly americké úřady dělat, pokud by je o jejich „superklíč" požádali například čínští policejní vyšetřovatelé?

Jak je tedy vidět, deontologický přístup k morálnímu dilematu okolo Farookova iPhonu s sebou nese kontroverze, které by mohly ústit ve střet různých institucí nebo přinášet problémy vycházející z potřeby nějak hierarchizovat kolidující hodnoty (resp. vytvořit precedent). Tyto okolnosti, jež mohou být předmětem obecné kritiky deontologie, jsou však v případě technologií zvláště posílené, a to proto, že zde mohou hrát roli projevy rozdílu mezi materiální a nemateriální částí kultury — tzv. kulturní lag.[25] Ona materiální část (technologie) se totiž vyvíjí rychleji než nemateriální (mj. mravní normy), a ta se kvůli tomu může stát dysfunkční, protože již nedokáže sloužit přiměřené strukturaci reality.[26] Z tohoto důvodu lze tedy o adekvátnosti některých povinností (případně práv) vztažených k posuzování etických otázek obklopujících technologie pochybovat, protože tyto povinnosti v době své formulace a institucionálního ukotvení s dotyčnou technologií a její rolí ve společnosti v nejmenším nepočítaly. Otázkami vyplývajícími z takto postavené námitky tedy je, nakolik deontologický přístup celý problém redukuje a zdali je „zvolená analogie" adekvátní. Prakticky se totiž nejedná o nic jiného než o použití argumentačního schématu založeného na analogickém vztahu (prohledat Farookův iPhone je jako prohledat jeho dům).

Historická perspektiva a možnost alternativního řešení

Při posuzování pře mezi Applem a FBI je jednou z okolností, která by měla být zmíněna, i historická perspektiva. Spor o paradigma zabezpečení informačních systémů (bezpečnost prostřednictvím přístupu vs. bezpečnost prostřednictvím neprostupnosti) se totiž odehrával už v mezidobí od poloviny let sedmdesátých a konce let devadesátých[27] a explanace jeho vývoje je něco, co může dobře posloužit ke komplexnějšímu pochopení zde probírané situace.

Problematika regulace šifrování může být datována např. od roku 1974, kdy v USA začala vznikat standardizovaná šifra DES, jež měla sloužit pro civilní účely (např. pro síťové komunikace bank). Její

[24] Viz Solon, Olivia. Hacking group auctions 'cyber weapons' stolen from NSA. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group>.

[25] Ogburn, William, F. *Social Change with Respect to Culture and Origin Nature*. New York: B. W. Huebsch, Inc.,1923. Teorie kulturního lagu je současnou sociologií za svůj technodeterminismus často kritizována – např. Meyrowitz, Joshua. Všude a nikde: Vliv elektronických médií na sociální chování. Praha: Karolinum, 2006.

[26] Ibidem.

[27] Levy, Steven. *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age*. New York: Penguin Books, 2001.

finální verze uvolněná v roce 1977 však byla zásluhou NSA kompromitována[28] (resp. kompromitovatelná[29]). Tato skutečnost nicméně do konce devadesátých let nebyla veřejně známá, a tím, co celou debatu v popisovaném období rámovalo byly především vládní regulace na vývoz šifrování, které jeho sílu omezovaly na úroveň 40bitového klíče[30], což se dokonce týkalo i publikací vědecké práce.[31] Takto nastavená politika se však začala drolit s příchodem devadesátých let, kdy se počítače staly masovou záležitostí a šifrování jako nedílná součást síťové komunikace nabylo na důležitosti. Incidentem charakteristickým pro počátek eroze americké „kryptopolitiky" se pak například stala aféra okolo garážového programátora Paula Zimmermana, který v roce 1991 na internet umístil volně stažitelný šifrovací nástroj používající 128bitový klíč. V očích zákona se z něj tak přes noc stal ilegální obchodník se zbraněmi a jeho několik let se táhnoucí případ nakonec skončil až knižním vydáním zdrojového kódu dotyčného programu (to je chráněno prvním dodatkem americké ústavy)[32]. Tím, co zapříčinilo konec plošného omezování kryptografie však byla především kauza okolo SSL.[33] V polovině devadesátých let se totiž začínalo výrazně prosazovat odvětví e-commerce a regulací redukované šifrování, které sloužilo například k zabezpečení internetových transakcí, se ukázalo jako nedostatečné (v roce 1995 bylo prolomeno). V roce 1996 tak byly americké exportní regulace přímo ústící ve zmenšující se zájem o tamní technologickou produkci[34] prezidentským dekretem velmi výrazně zmírněny.

Kromě přístupu, který by sílu šifrování omezoval — řekněme — plošně, se však ze strany amerických úřadů v devadesátých letech objevila i snaha o určitý kompromis. A tím byla právě metoda „superklíče", kterou tehdy zosobňoval tzv. Clipper chip. V plánu totiž bylo, aby tento šifrovací/dešifrovací čip z provenience NSA byl umisťován do nově vyráběných elektronických zařízení, jimž by poskytoval ochranu silné asymetrické šifry, což by však bylo vykoupeno existencí „zadních vrátek", k nimž by právě NSA měla přístup. Takovýto — v pojetí exekutivy — win-win scénář, však znovu narazil na odpor, přičemž hlavní protiargumenty směřované ze strany soukromého sektoru byly opět ekonomického charakteru: Mohl by produkt osazený Clipper chipem uspět na zahraničních

[28] Johnson, Thomas, R. *American Cryptography During the Cold War, 1945-1989: Book III:Retrenchment and Reform, 1972-1980*. Fort Meade: Center For Cryptologic History, Nacional Security Agency, 1998.

[29] Whitfield, Diffie – Hellman, Martin, E. Exhaustive Cryptanalysis of the NBS Data Encryption Standard. *Stanford.edu* [on-line] 1977 [cit. 5. 3.2019]. Dostupné z: <https://www-ee.stanford.edu/~hellman/publications/27.pdf>.

[30] Grimmett, Jeane, J. Encryption Export Control. [on-line] 2001 [cit. 5. 3.2019]. Dostupné z: <https://fas.org/irp/crs/RL30273.pdf>.

[31] Abelson, Harold et al. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. [on-line] 2015 [cit. 5. 3.2019]. Dostupné z: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>.

[32] Levy, Steven. *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age*. New York: Penguin Books, 2001.

[33] Ibidem.

[34] Ibidem.

trzích?[35] V polovině roku 1994, kdy byla v technologii čipu navíc objevena fatální bezpečnostní chyba, tak federální vláda z celého projektu začala pomalu couvat.

**Závěr**

Spor mezi společností Apple a FBI představoval faktický „morální horror" vycházející z dilemat uvozených dnešní podobou kryptografie. Původně vojenská technologie se totiž stala předmětem masového civilního užití, a to, jak se ukázalo, způsobilo ohrožení bezpečnosti, jelikož například zločinci takto získávají možnost využívat „neproniknutelnou digitální pevnost". Na druhou stranu zde ovšem existuje i perspektiva, v rámci níž soudobá kryptografie představuje důležitý bezpečnostní mechanismus, který chrání finance, identity a integritu komunikací obecně, a proto spor mezi Applem a FBI může být vnímán jako srážka těchto dvou náhledů. To, že každá z koncepcí bezpečnosti, která se v tomto sporu střetla, byla navíc podepřena i odlišným etickým schématem, pak nabízí poměrně unikátní možnost vzájemně porovnat implikace těchto normativních východisek ve vztahu k hodnocení dilemat uvozených technologií.

V rámci takovéto okolnosti — se zřetelem k probíranému sporu — pak byla předložena kritika deontologického přístupu stavějící na dvou tezích. Zaprvé na obtížnosti konceptualizace rámce východiska, na němž je založena povinnost (příp. právo) a zadruhé na aplikaci teorie kulturního lagu, což dohromady deontologický přístup ukazuje jako reduktivní historismus zacházející pouze s argumentací analogickou situací. Navíc však byla přednesena i historická paralela, z níž je patrné, že spor o regulaci kryptografie bohužel nemá uspokojivé alternativní řešení a že jsou zde navíc podstatné aspekty, které mluví proti pozici, jíž v probíraném sporu zastávala FBI. I pokud by totiž šifrování nějaké konkrétní služby/produktu bylo redukováno, zpravidla by se našla alternativa a celé opatření by tak z časového hlediska účinkovalo pouze v jediném případě, přičemž pozitivní potenciál by byl okamžitě vypotřebován a ten negativní by přetrvával. Kromě tohoto je však třeba zmínit i eventualitu vedlejších ekonomických škod, které by dnes — vzhledem k míře penetrace ICT — byly větší než tehdy.

Závěrečná teze odrážející předložené tak musí být doporučením ohledně nevhodnosti aplikace deontologických přístupů v otázkách bezprecedentních technologiemi uvozených dilemat. U tohoto apelu je však třeba zdůraznit, že v relaci ke zde probíraným souvislostem se týká především případů, jež dosud nenastaly. Utilitaristické (resp. negativně-utilitaristické) posouzení unikátních situací se totiž může stát dobrým základem pro formulaci v budoucnu adekvátních práv a povinností.

**Kontakt na autora:**

Radek Návrat, Teorie a dějiny vědy, Filozofická fakulta Masarykovy univerzity

email: 361948@mail.muni.cz

[35] Ibidem.

**Literatura**


Abelson, Harold et al. *Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications*. [on-line] 2015 [cit. 5. 3.2019]. Dostupné z: <https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>.

AP. Senator reveals that the FBI paid $900,000 to hack into San Bernardino killer's iPhone. *CNBC* [on-line] 2017 [cit. 5. 3.2019]. Dostupné z: <https://www.cnbc.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html>.

Borger, Julian. San Bernardino shooters radicalized as early as 2013, says FBI head. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/us-news/2015/dec/09/no-evidence-san-bernardino-attackers-part-of-wider-cell-loretta-lynch>.

CBS NEWS. CBS News poll: Americans split on unlocking San Bernardino shooter's iPhone. *CBS News* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.cbsnews.com/news/cbs-news-poll-americans-split-on-unlocking-san-bernardino-shooters-iphone/>.

Comey, James, B. Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?. *FBI.gov* [on-line] 2014 [cit. 5. 3.2019]. Dostupné z: <https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course>.

Comey, James. We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead. *Lawfare* [on-line] 2016 [cit. 5. 3.2018]. Dostupné na: <https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>. follow-lead>

Cook, Tim. A Message to Our Customers. *Apple* [on-line]2016 [cit. 5. 3.2019]. Dostupné z: <https://www.apple.com/customer-letter/>.

Gotlieb, Calvin, C. Privacy: A Concept Whose Time Has Come and Gone. In *Computers, Surveillance, and Privacy*. Lyon, David – Zureik, Elia (eds.). Minneapolis: University of Minnesota Press, 1997, s. 156–175.

Grimmett, Jeane, J. *Encryption Export Control*. [on-line] 2001 [cit. 5. 3.2019]. Dostupné z: <https://fas.org/irp/crs/RL30273.pdf>.

Himma, Kenneth Einar. Ethical Issues Involving Computer Security: Hacking, Hacktivism, and Counterhacking. In *The Handbook of Information and Computer Ethics.* Himma, Kenneth Einar (ed.). Londýn: Jones and Bartlett, 2007, s. 191–219.

Ingram, John, H. *Edgar Allan Poe: His Life, Letters, and Opinions*. Londýn: W. H. Allen And Co., 1886.

Johnson, Thomas, R. *American Cryptography During the Cold War, 1945-1989: Book III:Retrenchment and Reform, 1972-1980*. Fort Meade: Center For Cryptologic History, Nacional Security Agency, 1998.

Levy, Steven. *Crypto: How the Code Rebels Beat the Government — Saving Privacy in the Digital Age*. New York: Penguin Books, 2001.

Meyrowitz, Joshua. *Všude a nikde: Vliv elektronických médií na sociální chování*. Praha: Karolinum, 2006.

Nakashima, Ellen. FBI paid professional hackers one-time fee to crack San Bernardino iPhone. *Washington Post* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.washingtonpost.com/world/national-security/fbi-paid-professional-hackers-one-time-fee-to-crack-san-bernardino-iphone/2016/04/12/5397814a-00de-11e6-9d36-33d198ea26c5_story.html?utm_term=.b09b1af01648>.

Narayanan, Arvind. *What Happened to the Crypto Dream?, Part 1*. *IEEE.org* [on-line] 2013. [cit. 10. 3.2019]. Dostupné z: <http://ieeexplore.ieee.org/document/6493328/>.

Ogburn, William, F. *Social Change with Respect to Culture and Origin Nature*. New York: B. W. Huebsch, Inc.,1923.

Pym, Sheri. ORDER COMPELLING APPLE, INC. TO ASSIST AGENTS IN SEARCH [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.documentcloud.org/documents/2714001-SB-Shooter-Order-Compelling-Apple-Asst-iPhone.html>.

Solon, Olivia. Hacking group auctions 'cyber weapons' stolen from NSA. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/technology/2016/aug/16/shadow-brokers-hack-auction-nsa-malware-equation-group>.

Spafford, Eugene, F. Are Computer Hacker Break-ins Ethical? In *Internet Security: Hacking, Counterhacking, and Society*. Himma, Kenneth Einar (ed.). Londýn: Jones and Bartlett, 2007, s. 49–61.

Tavani, Herman. The Conceptual And Moral Landscape of Computer Security. In *Internet Security: Hacking, Counterhacking, and Society*. Himma, Kenneth Einar (ed.). Londýn: Jones and Bartlett, 2007.

Thompson, Paul, B. Privacy, Secrecy and Security. *Ethics and Information technology*, roč. 3, č. 1, 2001, s. 13–19.

US LEGAL. *All Writs Act Law and Legal Definition*. [on-line] nedat. [cit. 5. 3.2019]. Dostupné z: <https://definitions.uslegal.com/a/all-writs-act%20/>.

Whitfield, Diffie – Hellman, Martin, E. Exhaustive Cryptanalysis of the NBS Data Encryption Standard. *Stanford.edu* [on-line] 1977 [cit. 5. 3.2019]. Dostupné z: <https://www-ee.stanford.edu/~hellman/publications/27.pdf>.

Wilkinson, Tracy, L. *GOVERMENT'S STATUS REPORT*. [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.scribd.com/doc/306202728/FBI-apple-20160328#from_embed>.

Wilkinson, Tracy, L. *MEMORANDUM OF POINTS AND AUTHORITIES*. [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.documentcloud.org/documents/2773542-031123152171.html#document/p3>.

Yardon, Danny et al. Inside the FBI's encryption battle with Apple. *The Guardian* [on-line] 2016 [cit. 5. 3.2019]. Dostupné z: <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple