Triangulární vztah mezi ochranou lidských práv, kontrolou vývozu a technologiemi kybernetického dohledu

Ondřej Svoboda*

Triangular relationship among human rights protection, export controls, and cyber-surveillance technologies

Summary: *Recently, we are witnessing the rapid proliferation of cyber-surveillance technologies. Their misuse poses a threat to international security, as well as the protection of human rights and freedoms. Considerations given to the introduction of their effective protection on the one hand and legitimate cross-border commercial and technological export-based collaboration on the other hand lead to the complex triangular relationship. In order to provide effective and systematic export controls over sensitive emerging technologies to authoritarian states, it is necessary to set a rulebook, which goes beyond heavy-handed regulation conducted by the government. The private sector should espouse self-regulation based on due diligence principles and in compliance with the OECD Guidelines on Multinational Enterprises and the UN Guiding Principles on Business and Human Rights.*

Keywords: *Cyber-surveillance technologies; human rights; due diligence; export controls; dual-use goods; Wassenaar Arrangement; European Union*

Digitalizace společnosti a ekonomiky probíhá po celém světě s mimořádnou rychlostí. Nevyhýbá se ani obchodním společnostem, které na tom v některých případech profitují s vážnými společenskými dopady, včetně potenciálního vážného porušování lidských práv způsoby, které byly díky technologickému pokroku stěží představitelné před několika lety. Nové technologie například filtrují informace, a tak mohou zasahovat do svobody slova, stejně jako porušovat právo na soukromí. Tyto technologie jsou vyvíjeny a používány informačními a komunikačními technologickými (ICT) společnostmi, z nichž některé se staly platformami pro přístup k informacím, jejich sdílení, vyjadřování názorů a diskuze. Podle Výboru pro právní otázky a lidská práva Rady Evropy „se v několika zemích vytvořil obrovský ‚sledovací průmyslový komplex', který oslabuje demokratickou kontrolu a odpovědnost a ohrožuje svobodnou a otevřenou charakteristiku našich společností."[1] Tento stav je tak úzce provázán s obchodními zájmy firem, stejně jako s bezpečnostními zájmy států. Samozřejmě platí, že technologie kybernetického dohledu, kam typicky patří všechny technologie umožňující sledování, jako je odposlech mobilních telekomunikací nebo rušící zařízení; software umožňující průnik do systému; systémy nebo zařízení pro dohled nad komunikačními sítěmi IP; software navržený nebo upravený speciálně pro sledování nebo analýzu donucovacími orgány, mohou mít legitimní využití. V rukou některých států se ale staly nástrojem pro rozsáhlé porušování lidských práv, vnitřní represe a potlačování občanské společnosti, včetně pronásledování novinářů, disidentů nebo obhájců lidských práv. Technologický vývoj ve spojení s obchodními zájmy proto představuje vážnou normativní výzvu pravidlům na vnitrostátní i mezinárodní úrovni.

Závažné důsledky kontroly kyberprostoru a internetu lze sledovat každý den. Ukázkovým příkladem je omezení toku informací z Číny při vypuknutí pandemie covidu-19, kdy čínská vláda použila všechny dostupné nástroje k monitorování a řízení diskuze na čínské části internetu.[2] Podobně byly sledovací technologie využívány ji dříve při tzv.

* Autor působí na katedře mezinárodního práva PF UK a na velvyslanectví ČR v Tokiu. Názory obsažené v tomto článku jsou pouze osobními názory autora a nevyjadřují oficiální stanovisko Ministerstva zahraničních věcí ČR. Článek vznikl v rámci projektu COOP – Cooperation. E-mail: ondrej.svobod@gmail.com.

1 Council of Europe. *Mass surveillance Report*. Doc. 13734, 2015, str. 1.

2 Amnesty International. *EU companies selling surveillance tools to China's human rights abusers*. [online]. 21. 9. 2020. Dostupné na <https://www.amnesty.org/en/latest/news/2020/09/eu-surveillance-sales-china-humanrights-abusers/>; KHALIL, L. Digital authoritarianism, China and covid. In: *Lowy Institute* [online]. 2. 11. 2020. Dostupné na <https://www.lowyinstitute.org/publications/digital-authoritarianism-china-and-covid>.

arabském jaru, kdy zvláště americké a evropské technologie pomáhaly autoritářským režimům při potlačování vnitřní opozice.[3] Další příklady nabízí uplatňování technologií Ericssonu v Bělorusku nebo Nokia Siemensu v Íránu.[4] Nejnověji poutá pozornost demokratických států situace v čínské autonomní oblasti Sin-ťiang, kde se poslední roky buduje účinný sledovací systém za aktivního technologického přispění západních společností.[5] Uvedené případy vyvolávají otázky, zda neadekvátní nástroje ke kontrole exportu technologií kybernetického dohledu neumožnily „rychlý rozvoj soukromých společností, které dodávají takové technologie vládám po celém světě, někdy bez ohledu na lidskoprávní dopady".[6]

Technologický vývoj do značné míry utváří schopnost jednotlivců vykonávat jejich právo na svobodu projevu a jiné svobody. Tento vývoj také vyžaduje nová pravidla na mezinárodní, regionální i vnitrostátní úrovni. Podle zvláštního zpravodaje Rady OSN pro lidská pro podporu a ochranu svobody vyjadřování a projevu je situace natolik vážná, že by nemělo zůstat pouze u přísnější regulace vývozu technologií kybernetického dohledu a omezení k jejich užití, ale mělo by být vyhlášeno okamžité moratorium na celosvětový prodej a transfer nástrojů sledování, dokud nebudou zavedeny lidskoprávní pojistky.[7]

Právní úprava vývozu technologií kybernetického dohledu ale vyvolává řadu otázek také pro obchodní společnosti, které se jejich vývojem a prodejem zabývají. Dodržování pravidel kontroly vývozu může být náročné, co se týče kapacit i času, než se podaří v procesu vydávání licencí povolení získat, a to zvláště pro menší společnosti. Dlouhé čekací lhůty a složité administrativní procesy mohou nakonec vést k uniklým obchodním příležitostem, kdy zakázku získá rychlejší konkurence. Negativní přímý dopad kontroly vývozu na odvětví nových technologií byl již také zdokumentován.[8] Nalezení žádoucí rovnováhy mezi protichůdnými zájmy je tak pro regulátory velice obtížné.

Cílem tohoto příspěvku je přiblížit problematiku triangulárního vztahu soukromých společností, států a jednotlivců a jak v něm hledat rovnováhu mezi obchodními, hospodářskými a lidskými právy v kontextu vývozu technologií kybernetického dohledu. Komplexnost těchto vztahů vychází z otázky nad regulační rolí státu a obchodními zájmy soukromého sektoru. Střet těchto dvou světů samozřejmě není ničím novým, zvláště pro oblast kontroly vývozu, kdy je obchodování s některými nebezpečnými materiály jako azbest nebo nebezpečné chemikálie přísně regulováno. V souvislosti se svobodou projevu je zde pak střet státu jako zákonodárce a garanta základních práv a svobod a jeho další rolí, která podporuje inovační a průmyslový růst a v rámci něj pomáhá růstu vlastních obchodních společností a jejich prosazování na zahraničních trzích.

Přísná kontrola technologií vytvářejících sledovací systémy, zasahujících do soukromí lidí a vyvážených do zahraničí může pomoci zabránit jejich zneužití k porušování lidských práv a pro jiné nelegitimní účely. Nicméně je třeba si také uvědomit, že digitální technologie mohou stejně tak vytvářet v zemích, do kterých směřují, nové ekonomické příležitosti, a podpořit tak hospodářský rozvoj, růst životní úrovně, a tak i nastolit dilema mezi krátkodobou ochranou určitých občanských a politických práv a rozvojem hospodářských a sociálních práv v dlouhodobém horizontu.[9]

Všechny uvedené trendy ještě umocňuje rychlý rozvoj digitalizace. Vlády experimentují s novými digitálními službami pro občany, vytvářejí jim digitální identity a sdílejí v digitálním prostředí bezprecedentní množství osobních údajů. Především pak ve stále více digitálním světě narůstá počet běžných každodenních aktivit, které se odehrávají online.

Tento příspěvek tak nejdříve nabídne právní analýzu dopadu digitálních technologií na svobodu projevu a související práva, která jsou součástí univerzálního systému ochrany lidských práv. Následuje část věnující se Waasenarskému ujednání, multilaterálnímu mezinárodnímu režimu, který reguluje obchod se zbožím dvojího užití. Tento systém kontroly vývozu nicméně dostatečně nezohledňuje technologický pokrok oproti nedávnému posunu na úrovni Evropské unie, který bude přiblížen v další části. Na základě toho

3 European Parliament. *After the Arab Spring: new paths for Human Rights and the Internet in European Foreign Policy*. 2012, str. 9–10.
4 WAGNER, B. *Exporting censorship and surveillance technology*. Humanist Institute for Co-operation with Developing Countries, 2012, str. 7.
5 Sinopsis. *Globalizace sledovacích technologií*. 25. 4. 2021.
6 CAPONETTI, L. Mass surveillance technology: trading Trojan Horse?. *Strategy Trade Review*, 2016, sv. 2, č. 2, str. 70.
7 Human Rights Council. *Surveillance and human rights: report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. 2019, A/HRC/41/35, odst. 66a.
8 Např. EZELL, S. — FOOTE, C. How stringent export controls on emerging technologies would harm the U.S. In: *Economy, Information Technology & Foundation* [online]. 20. 5. 2019. Dostupné na <https://itif.org/publications/2019/05/20/how-stringent-export-controls-emerging-technologies-would-harm-us-economy>.
9 KANETAKE, M. The EU's dual-use export control and human rights risks: the case of cyber surveillance technology. *Europe and the World: Law Revue*, 2019, sv. 3, č. 1, str. 15.

bude představen nový regulační rámec, který by měl být postaven na chytrém mixu mezinárodních standardů, náležité péči pro dodržování lidských práv a soukromé samoregulaci. V závěru článek doporučuje, aby se k dosažení rovnováhy mezi lidskými právy, obchodními zájmy a technologickým rozvojem přistoupilo k aktualizaci pravidel kontroly vývozu ve spojení s implementací standardů náležité péče.

Dopad obchodních aktivit společností ICT na lidská práva v digitální sféře

Společnosti ICT vyvinuly širokou škálu nástrojů k řízení a sledování aktivit v kyberprostoru. Jedná se např. o odposlechy, rušicí zařízení, průniky do systémů a databází, automatické upozorňování, odstraňování a filtrování před zveřejněním. K vyhodnocování rostoucího množství získaných informací navíc vytváří automatizované postupy, stále častěji založené na algoritmech využívajících umělou inteligenci (AI). To vše vyvolává obavy nad souladem jejich masivního použití s lidskoprávními standardy. Vývoj a používání těchto technologií navíc ve většině případů postrádá transparentnost a jsou dostupné pouze omezené množství informací pro veřejnou kontrolu a možná nápravná opatření. Řada pozorovatelů i upozorňuje na technologicky vyspělé mechanismy cenzury a sledování, které jsou navrženy k porušování lidských práv, pro něž lze jen obtížně nalézt v jejich systematickém použití legitimní či zákonné důvody.[10]

Vzrůstající obavy potvrdili i zvláštní zpravodajové Organizace pro bezpečnost a spolupráci v Evropě (OBSE) v r. 2017. Dle jejich stanoviska svoboda vyjadřování se vztahuje i na internet a „zablokování webových stránek, IP adres, portů, síťových protokolů nebo jiných uživatelských spojení (jako sociální sítě) je extrémním opatřením", které může být jedině ospravedlnitelné, pokud je v souladu s mezinárodními standardy. Dále zpravodajové upozornili, že „mechanismy filtrování podle obsahu, které neovládají koneční uživatelé, jsou nástrojem cenzury a jako takové nejsou ospravedlnitelným omezením svobody vyjadřování".[11] Je tak evidentní, že obchodní aktivity společností ICT mohou mít přímý negativní dopad na ochranu soukromí, práva na práva na důstojný, soukromý a rodinný život, svobodu projevu, slova či právo shromažďovací, sdružovací a účastnit veřejného života. Tato práva jsou navíc vzájemně provázána a na sobě závislá, především pak ve stále více digitálním světě, kde narůstá počet našich aktivit, které se odehrávají online. Právo na soukromí je např. nezbytné pro naplnění svobody vyznání,[12] nebo – slovy zvláštního zpravodaje OSN pro podporu a ochranu práva na svobodu názoru a svobodu projevu – „zasahování do soukromí skrz cílené sledování je navrženo k potlačování užívání svobody projevu".[13] V souladu s takovým pohledem se tento článek především zaměřuje na právo na svobodu projevu a přiznává ostatním svobodám nedělitelnou úlohu při jeho výkonu.

V tomto kontextu je nutné připomenout zvláště čl. 19 Univerzální deklarace lidských práv a čl. 19 Mezinárodního paktu o občanských a politických práv (ICCPR), protože představují základní výchozí bod při analýze mezinárodního rámce. Tato ustanovení totiž chrání právo každého na svobodu přesvědčení a projevu a zahrnuje právo vyhledávat, přijímat a rozšiřovat informace a myšlenky jakýmikoli prostředky a *bez ohledu na hranice*. Toto právo také zahrnuje povinnost státu zajistit prostředí, které to umožní, jako např. ve formě nezávislých a rozmanitých médií a svobodného přístupu k informacím.[14]

Ve vztahu k vývozcům technologií kybernetického dohledu a dalším soukromým osobám Obecné zásady OSN pro byznys a lidská práva (dále jen „Obecné zásady OSN"), přijaté v r. 2012, předepisují státům přijmout vhodné kroky, které zajistí ochranu před porušováním lidských práv třetími stranami včetně podniků. To je také v souladu se závěry Výboru pro lidská práva v jeho obecném komentáři č. 31 k ICCPR na téma možností porušení ICCPR „neschopností přijmout vhodná opatření k výkonu náležité péče k zabránění, potrestání, prošetření a nebo nápravy škody" způsobené soukromými subjekty.[15] Ke splnění této povinnosti je tak od států

10 WAGNER, c. d., str. 7.
11 Organization for Security and Co-operation in Europe. *Joint declaration on freedom of expression and "Fake News, Disinformation and Propaganda"*. 3. 3. 2017.
12 Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. 2015, UN DOC A/HRC/29/32, odst. 16–18.
13 Human Rights Council. *Surveillance and human rights: report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. 2019, A/HRC/41/35, odst. 21.
14 Organization for Security and Co-operation in Europe. c. d., část 3. Viz také Human Rights Committee. *General Comment No. 34 on the freedoms of opinion and expression*. 2011, UN DOC CCPR/C/GC/34, odst. 18, 40.
15 Human Rights Committee. *General Comment No. 31: Nature of the Legal Obligation Imposed on States Parties to the Covenant*. 2004, UN DOC CCPR/C/21/Rev.1/Add. 13, odst. 8.

očekáván odpovídající dohled nad aktivitami osob podléhajících jejich jurisdikci nebo legislativní aktivita k vytvoření takových podmínek, které povedou společnosti k dodržování lidských práv.[16] I zde ovšem stejně jako v řadě jiných případů platí, že uvedení do praxe není jednoduché. Může být navíc sporné, zda se obecná doporučení k náležité péči vztahují i na státní orgány regulující vývoz do jejich zemí, obzvláště pokud neexistuje přímá vazba mezi obchodními aktivitami v zahraničí a porušováním ICCPR.[17] Další možnou překážkou může být úzký výklad čl. 2 ICCPR, kdy závazky z něj vyplývající pro státy se vztahují na jednotlivce, které má stát na svém území a území podléhajícím jeho jurisdikci.

Výklad působnosti ICCPR se nicméně může vyvíjet. To potvrzuje doporučení Výboru pro lidská práva v jeho hodnoticí zprávě k Itálii z r. 2017 ke změnám v pravidlech kontroly vývozu. Výbor vyjádřil své znepokojení nad „obviněními, že společnosti mající sídlo ve smluvní straně poskytují vybavení pro online sledování vládám, které se dopouštějí závažného porušování lidských práv, a chybějícími právními pojistkami nebo mechanismem dohledu, co se týče vývozu takového vybavení" a doporučil přijmout opatření k „zajištění, že všechny podniky podléhající její jurisdikcí, zvláště technologické podniky, budou dodržovat lidskoprávní standardy při obchodních aktivitách v zahraničí".[18] Z doporučení lze vyvodit směřování k rozšíření působnosti ICCPR a jeho aplikaci při lidskoprávní náležité péči, a to i konkrétně ve vztahu k licenčnímu řízení při vývozu informačních technologií.[19]

Je důležité si také uvědomit, že spolupráce mezi vývozci a státy, které odebírají sledovací a cenzurující technologie, často nekončí momentem prodeje. Společnosti ze sektoru ICT v řadě případů poskytují i následnou podporu těmto systémům, včetně údržby a aktualizací. V r. 2014 tak např. britsko-německá společnost FinFisher, vyvíjející sledovací software, měla uzavřené smlouvy s několika vládami, ve kterých se zavázala poskytovat v různé podobě zákaznickou podporu.[20] Tato forma dlouhodobé spolupráce mezi veřejným a soukromým sektorem vnáší další pochybnosti, zda je ze strany společnosti dodržována základní náležitá péče zohledňující dopady na lidská práva, zvláště v rizikových regionech. Pochybnosti jsou ale také nad prováděnými kontrolami státními orgány v oblasti lidských práv a náležité péče v procesu vydávání vývozních licencí.

Je realitou, že autoritářské režimy po celém světě používají nejnovější nástroje na kontrolu internetu a komunikačních aplikací. Snaží se nejen o omezení šíření informací o protivládních protestech, ale i o potlačení svobody projevu a o rozšíření dosahu státní moci za dosavadní hranice.[21] Pravděpodobně nejrozvinutější sledovací infrastruktura se nachází v čínské provincii Sin-ťiang, kdy navíc využívá umělou inteligenci, rozpoznávání obličeje a kombinuje je se sledováním pohybu a chování. Podle americké vlády jsou tyto technologické systémy v Sin-ťiang dodávány a podporovány zahraničními společnostmi a investory.[22] Obchod s technologiemi kybernetického dohledu má na tomto stavu jistě nezanedbatelný podíl, protože na mezinárodních trzích dominují především technologie vyvinuté v USA a EU.[23]

Při vědomí toho, že různé vlády a režimy podnikají kyberútoky proti politickým oponentům, občanské společnosti, novinářům či blogerům za účelem sledování, vydírání, zastrašování, manipulace či zdiskreditování, vlamují se do jejich účtů na sociálních sítích, blokují nebo mažou jejich weby a blogy, je vztah mezi lidskými právy a vývozem informačních technologií nepopíratelný. Takové technologie mají totiž odrazující účinek a vážně narušují právo na svobodu pokojného shromažďování, svobodu projevu a veřejnou účast atd. Při systematickém používání navíc mohou vést k odstranění demokratické kontroly a podkopávání právního státu. Jsou však nástroje kontroly vývozu nejvhodnější a nejúčinnější odpovědí?

Wassenaarské ujednání

Regulace a kontrola vývozu upravuje vývoz, dovoz a přepravu některého méně citlivého

16 Human Rights Council. *Report of the Office of the United Nations High Commissioner for Human Rights on the seminar on experiences of archives as a means to guarantee the right to the truth*. 2011, UN DOC A/HRC/17/21, zásada č. 3.
17 KANETAKE, *The EU's dual-use export*, str. 12.
18 Human Rights Committee. *Concluding observations on the Sixth Periodic Report of Italy*. 2017, UN DOC CCPR/C/ITA/CO/6, odst. 36–37.
19 KANETAKE, M. Converging Dual-Use Export Control with Human Rights Norms: The EU´s Responses to Digital Surveillance Exports. In: Fahey, E. (ed.). *Framing Convergence with the Global Legal Order*, London 2020, str. 77.
20 Privacy International, c. d.
21 WAGNER, c. d., str. 12.
22 US Department of State. *Guidance on implementing the "UN Guiding Principles" for transactions linked to foreign government end-users for products or services with surveillance capabilities*. 2020; US Department of State. *Xinjiang supply chain business advisory: risks and considerations for businesses with supply chain exposure to entities engaged in forced labor and other human rights abuses in Xinjiang*. 2020, str. 4.
23 Situace se nicméně mění a Čína se stává významným dodavatelem sledovacích technologií, a tak i globálním hráčem pro šíření tzv. autoritářských technologií (*authoritarian tech*). FELDSTEIN, S. *The global expansion of AI surveillance*. Carnegie Endowment, 2019, str. 13.

vojenského materiálu a tzv. zboží a technologie dvojího užití, tj. široká škála produktů tradičně v průmyslové, jaderné, chemické a biologické oblasti, které jsou primárně vyráběny a předurčeny pro civilní použití, ale mohou být vzhledem ke svému charakteru a vlastnostem použity i pro vojenské účely. Státní orgány jsou s ohledem na bezpečnostní zájmy oprávněny k posuzování, vyhodnocování a vyřizování žádostí o vydání povolení a licencí.

Původně kontrolní režimy nebyly navrženy jako nástroje k regulaci technologií kybernetického dohledu. Nicméně potřeba držet krok s někdy až překotným technologickým pokrokem vyvolala diskuzi, jak to reflektovat a jak do seznamů kontrolovaných položek zahrnout nové digitální technologie. Nejviditelnějším příkladem těchto snah je vývoj v rámci Wassenaarského ujednání o vývozních kontrolách konvenčních zbraní a zboží a technologií dvojího užití, které je pravděpodobně nejširší z mezinárodních kontrolních režimů. Wassenaarské ujednání je mezinárodní dohoda, která v současné době sdružuje 44 zemí – významných výrobců a vývozců zbraní, jejímž cílem je posilování transparentnosti a zvyšování odpovědnosti v mezinárodním obchodu s konvenčními zbraněmi a zbožím dvojího použití.[24] K naplňování tohoto cíle se smluvní státy zavazují ke kontrole vývozu položek uvedených na jeho seznamech.

Rostoucí obavy spojené s vývozem citlivých technologií vedly k tzv. kyberdodatku,[25] seznamu s cílem „zabránit šíření aktivních nebo útočných kybertechnologií, které jsou používány k zahájení kyberútoků nebo aktivně získávají a analyzují chráněné údaje".[26] V prosinci 2012 byl seznam aktualizován, aby zahrnoval technologie k odposlechu mobilní komunikace.[27] Následně o rok později, v prosinci 2013, byla provedena další aktualizace zařazující na seznam software k monitorování sítí a sběru dat.[28] Tyto kroky představovaly pozitivní precedent pro kontrolu vývozu kybertechnologií, zvláště v oblastech nástrojů pro sledování, a zohledňování lidskoprávních dopadů. V kontextu Wassenaarského ujednání se mj. jednalo i o „první důležité kroky k zavedení kontroly na multilaterální úrovni".[29]

Nicméně tento vývoj byl také od počátku vnímán z různých důvodů jako kontroverzní. Panovaly především pochybnosti, zda je Wassenaarské ujednání vhodným forem na zavedení tohoto typu vývozních omezení. V jeho zakládající listině, tzv. Výchozích prvcích *(Initial Elements)*, se lidská práva totiž vůbec nezmiňují. Tehdejší kritici, včetně USA, varovali před obecnými definicemi některých nových pojmů jako software umožňující tajné vniknutí do systémů („intrusion software"). Takové „pseudo-technické" pojmy podle kritiků otevíraly cestu k různým výkladům a ve svém důsledku by mohly mít negativní vliv i na technologie bránící sledování.[30] V tomto duchu skupina společností z ICT odvětví založila v červenci 2015 dokonce koalici proti implementaci nových kontrol kvůli jejich negativním dopadům na celosvětový výzkum a vývoj v digitálních technologiích.[31]

Účinnost Wassenaarského ujednání je také oslabena jeho nezávaznou povahou stejně jako chybějícími vodítky k jeho provádění a vynucovacím mechanismem. To dává státům značnou volnost v rozhodování, jestli a jak kontrolovat položky na seznamu.[32] Podle některých pozorovatelů se tak jedná o nevhodný mezinárodní rámec pro řešení hrozeb, které přestavuje digitální sledování pro lidská práva. Navíc provádění komplexní kontroly vývozu je náročné pro licenční orgány stejně jako pro exportéry kvůli specifickým charakteristikám ICT odvětví ve formě vysokého stupně přeshraniční spolupráce, množství mezinárodních týmů umístěných v různých částech světa, dlouhých dodavatelských řetězců, vedoucích zpravidla přes několik států, stejně jako propojenosti a vysoké

[24] Wassenarské ujednání má ze všech kontrolních režimů nejširší předmět své činnosti. Ten je definován 1) seznamem vojenského materiálu (pokrývající konvenční vojenský materiál) a 2) seznamem zboží dvojího užití technologií (jenž pokrývá položky, které nejsou zahrnuty do kontrolních listů ostatních kontrolních režimů). Podstatou činnosti Wassenarského ujednání je mezinárodní výměna informací o obecných aspektech mezinárodního obchodu se strategickým zbožím, mezi něž patří globální trendy obchodu se zbraněmi, bezpečnostní situace v určitých regionech, případně nákupní aktivity, projekty či firmy vzbuzující podezření z nelegálních transakcí apod.

[25] PYETRANKER, I. An umbrella in a Hurricane: cyber technology and the December 2013 amendment to the Wassenaar Arrangement. *Northwestern Journal of Technology and Intellectual Property*, 2015, sv. 13, č. 2, str. 162.

[26] REISER, D. – HINDIN, D. Caught by surprise: Israel's export control regime and cyber technologies. In: *World ECR* [online]. 20. 5. 2014. Dostupné na <https://www.worldecr.com/archive/caught-by-surprise-israels-export-control-regime-and-cyber-technologies/>.

[27] Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, WA-LIST (12) 1, 12. 12. 2012, Category 5.A.1.f.

[28] Wassenaar Arrangement, List of Dual-Use Goods and Technologies and Munitions List, WA-LIST (13) 1, 4. 12. 2013, Categories 4.A.5, 5.A1.j.

[29] BOHNENBERGER, F. The proliferation of cyber-surveillance technologies: challenges and prospects. *Strategy Trade Review*, 2017, sv. 3, č. 4, str. 84–85.

[30] DULLIEN a kol. *Surveillance, software, security, and export controls. Reflections and recommendations for the Wassenaar Arrangement Licensing and Enforcement Officers Meeting: Draft report*. 12. 10. 2015; BRATUS, S. a kol. Why Wassenaar arrangement's definitions of intrusion software and controlled items put security research and defense at risk – and how to fix it. In: *Dartmouth* [online]. 9. 10. 2014. Dostupné na <https://www.cs.dartmouth.edu/~sergey/wassenaar/wassenaar-public-comment.pdf 2014>.

[31] RUOHONEN, J. – KIMPPA, K. Updating the Wassenaar debate once again: surveillance, intrusion software, and ambiguity. *Journal of Information Technology & Politics*, 2019, sv. 16, č. 2, str. 184.

[32] PYETRANKER, c. d., str. 168.

dynamice tohoto sektoru.[33] Je vhodné také připomenout, že Čína není stranou ujednání, čímž se zásadně oslabuje dopad mnohostranného systému kontrol vývozu na sledovací technologie. Situace se stává ještě složitější, pokud se vezme v úvahu, že změna ustanovení Wassenaarského ujednání vyžaduje jednomyslnost. Tato slabina se naplno ukázala např. v r. 2016, kdy plenární zasedání nedokázalo přijmout změnu několika ustanovení reagujících na další technologický pokrok navzdory dvouletým přípravám a předběžné dohodě stran.[34]

Ačkoliv tak mnohostranné režimy, jakými jsou Australská skupina, Wassenaarské ujednání, Kontrolní režim raketových technologií, Skupina jaderných dodavatelů nebo Zanggerův výbor, zajišťují při kontrole vývozu jistou úroveň transparentnosti, předvídatelnosti a harmonizace jinak decentralizovaných národních přístupů,[35] jejich neschopnost rychle reagovat na nové technologické výzvy vedla v posledních letech k jednostranným iniciativám. Mezi ty nejvýznamnější lze řadit vývoj v EU.

Evropská unie v popředí přísnější kontroly

Diskuze o vývozu technologií kybernetického dohledu začala v EU nabývat na významu v průběhu arabského jara, kdy bylo prokázáno několik případů, kdy byly sledovací technologie evropských společností použity autokratickými režimy v severní Africe a na Středním východě k potlačování práv obyvatelstva. Evropské společnosti patří celosvětově mezi největší vývozce těchto technologií. Studie z r. 2015 zaznamenala přes 80 případů exportovaných sledovacích systémů z EU v situacích, kdy docházelo k porušování lidských práv nebo byla ohrožena mezinárodní či evropská bezpečnost.[36] Není proto překvapivé, že europoslanci, nevládní organizace i lidskoprávní aktivisté opakovaně požadovali změnu pravidel vývozu technologií dvojího užití a digitálního dohledu z členských zemí do zemí mimo EU, konkrétně rozšíření seznamu zboží dvojího užití, stejně jako zohlednění lidskoprávních dopadů v cílové zemi vývozu.[37]

Vedle mezinárodních režimů, které poskytují základní rámec pro jeho kontrolu vývozu, existují totiž také unijní pravidla uplatňující se při vývozu do třetích zemí. Ta byla v době arabského jara stanovena v nařízení Rady (ES) 428/2009, kterým se zavádí režim Společenství pro kontrolu vývozu, přepravy, zprostředkování, technické pomoci a tranzitu zboží dvojího užití.[38] Protože příslušné unijní nařízení bylo založeno na mnohostranných kontrolních režimech, průběžné změny v seznamu zboží dvojího užití Wassenaarského ujednání z let 2012 a 2013 se následně také odrazily v seznamu kontrolovaných položek EU v r. 2014.[39] Nicméně pro řadu pozorovatelů nenabízel tento systém založený na vyjednáváních v rámci Wassenaarského ujednání dostatečně účinnou kontrolu nad vyváženými technologiemi kvůli slabým stránkám Wassenaarského ujednání.

Z výše uvedených důvodů tak Evropský parlament v r. 2015 vznesl požadavek na revizi příslušného nařízení s cílem nastavit pravidla pro vývoz kybertechnologií, které mohou porušovat lidská práva ve třetích zemích.[40] Jen o několik týdnů později přijala také Rada Akční plán pro lidská práva a demokracii 2015–2019, ve kterém podpořila revizi nařízení Rady (ES) č. 428/2009 s cílem zmírnit potenciální rizika spojená s nekontrolovaným vývozem zboží v oblasti informačních a komunikačních technologií, které by bylo možné použít způsobem vedoucím k porušování lidských práv.[41]

Komise reagovala v září 2016 návrhem na zohledňování lidskoprávních dopadů do procesu povolování vývozu, což by podle jejího názoru zpřísnilo kontrolu nad vyváženými citlivými technologiemi.[42] Podle návrhu

33 BOHNENBERGER, c. d., str. 84.
34 THOMSON, I. Wassenaar weapons pact talks collapse leaving software exploit exports in limbo. In: *The Register* [online]. 21. 12. 2016. Dostupné na <https://www.theregister.com/2016/12/21/wassenar_negotiations_fail/>.
35 KANETAKE, M. Controlling the Export of Digital and Emerging Technologies. *Security and Human Rights*, 2021, sv. 31, str. 2.
36 ECORYS and SIPRI. *Final report: data and information collection for EU dual-use export control policy review*. 6. 11. 2015.
37 KRAHULCOVA, L. The European Parliament is fighting to strengthen the rules for surveillance trade. In: *Access Now* [online]. 8. 12. 2017. Dostupné na <https://www.accessnow.org/european-parliament-fighting-strengthen-rulessurveillance-trade>.
38 Nařízení Rady (ES) č. 428/2009 ze dne 5. května 2009, kterým se zavádí režim Společenství pro kontrolu vývozu, přepravy, zprostředkování a tranzitu zboží dvojího užití. Úř. věst. L 134, 29. 5. 2009, s. 1–269. V ČR implementováno zákonem č. 594/2004 Sb., jímž se provádí režim Evropských společenství pro kontrolu vývozu zboží a technologií dvojího užití.
39 Nařízení Komise v přenesené pravomoci (EU) č. 1382/2014 ze dne 22. října 2014, kterým se mění nařízení Rady (ES) č. 428/2009, kterým se zavádí režim Společenství pro kontrolu vývozu, přepravy, zprostředkování a tranzitu zboží dvojího užití.
40 Usnesení Evropského parlamentu ze dne 8. září 2015 o lidských právech a technologiích: dopad systémů narušování a sledování na lidská práva ve třetích zemích (2014/2232(INI)), odst. 35–39; viz také Usnesení Evropského parlamentu ze dne 22. listopadu 2016 o evropské obranné unii (2016/2052(INI)), odst. 21.
41 Závěry Rady o akčním plánu pro lidská práva a demokracii 2015–2019. 20. 7. 2015, b. 25(e).
42 Evropská komise. Návrh nařízení Evropského parlamentu a Rady, kterým se zavádí režim Unie pro kontrolu vývozu, přepravy, zprostředkování, technické pomoci a tranzitu u zboží dvojího užití (přepracované znění). COM(2016)616 final, 28. 9. 2016.

by orgány odpovědné za kontrolu vývozu měly zohlednit dodržování lidských práv v zemi určení při udělení licence. Navíc by seznam zboží dvojího užití zahrnoval novou kategorii pokrývající technologie kybernetického dohledu, které by šly i nad rámec užšího seznamu Wassenaarského ujednání. Dále Komise navrhla rozšířit rozsah nařízení o univerzální ustanovení.[43] To by umožnilo kontrolovat i vývoz technologií, které nejsou vedeny na seznamu. Zavedení lidskoprávního normativního kritéria však představovalo výrazný posun z tradičního pojetí kontroly vývozu[44] a sblížení kontroly s unijním závazkem k podpoře a implementaci Obecných zásad OSN.[45] Návrh navíc obsahoval změny klíčových pojmů. Především definice zboží dvojího užití byla revidována tak, aby odrážela vývoj nových kategorií zboží dvojího užití, jako jsou technologie kybernetického dohledu.

Návrh se však setkal s odporem, především motivovaným strachem ze ztráty konkurenceschopnosti. Uniklý dokument dokládal, že devět členských států kritizovalo navržený text a požadovalo menší váhu lidskoprávního kritéria.[46] Průmysl se také obával, že nová podoba nařízení by ohrozila jeho legitimní obchodní aktivity. Např. podle asociace unijního digitálního průmyslu DIGITAL EUROPE „by současná definice dvojího užití měla být zachována na základě mezinárodně zavedené definice."[47] Podobně Federace německého průmyslu varovala, že společnosti „nejsou v pozici, aby zaujímaly politické postoje".[48] Zástupci byznysu se tak bránili povinnosti provádět hodnocení lidskoprávních dopadů použití vyvážených technologií a jako vhodnější pro tuto roli viděli státy s jejich odborným byrokratickým aparátem.

Složitý legislativní proces byl nakonec uzavřen až v listopadu 2020 po několika letech vyjednávání a hledání kompromisu mezi unijními institucemi. Výsledné nařízení představuje současnou formu celoevropského rámce pro kontrolu vývozu. Mezi novými pravidly je zavedení přísnější kontroly nad vývozem technologií, které mohou za jistých okolností představovat riziko závažného porušování lidských práv, vnitřní represe a bezpečnosti konečným uživatelem. Je revidována definice „zboží dvojího užití", kdy je nově spojena s definicí „technologie kybernetického dohledu" a pozměněnými kritérii kontroly.[49] Zavádí se také první samostatný seznam kontrolovaných položek rozšířený o citlivé technologie. Tímto krokem se EU odpoutává od dosavadní úzké provázanosti s mnohostrannými mezinárodními režimy, především s Wassenaarským ujednáním, ale může na druhou stranu nezávisle rozhodovat o kontrole vývozu citlivých technologií. Podle zpravodajky Evropského parlamentu pro legislativu týkající se vývozu zboží dvojího užití Markéty Gregorové tento nový mechanismus „umožní překročit omezení daná Wassenaarem, jenž svým rozsahem a rychlostí přijímání beznadějně zaostává za současným technologickým pokrokem".[50]

Novelizace také posílila koordinační mechanismy mezi členskými státy, resp. jejich licenčními orgány navzájem, i členskými státy a Evropskou komisí, vymahatelnost pravidel, transparentnost procesu rozhodování o licencích a kolaboraci s třetími zeměmi v oblasti kontroly zboží dvojího užití. Větší pozornost je věnována i užšímu nastavení vztahů se soukromým sektorem prostřednictvím výukových programů a konzultací. To je rozhodně vítaný krok, protože spolehnutí se pouze na restrikce by nemělo kýžený efekt.

Dlouhý proces v EU[51] si zaslouží pozornost minimálně ze dvou důvodů. Zaprvé dokazuje, jak je obtížné najít rovnováhu mezi protichůdnými zájmy v kontrole vývozu sledovacích technologií. Zvláště v poslední době se pod vlivem Evropského parlamentu do priorit společné obchodní politiky EU stále častěji prosazují nekomerční zájmy a hodnoty.[52] Zadruhé nové nařízení má potenciál

43 Tzv. catch-all clause umožňuje v určitých situacích, kdy existuje důkaz, že může dojít ke zneužití, kontrolovat vývoz technologií, které nejsou uvedeny na seznamu.
44 KANETAKE, *The EU's dual-use export*, str. 7.
45 KANETAKE, *Converging Dual-Use Export*, str. 72.
46 Council of the EU. Paper for discussion – for adaption of an improved EU Export Control Regulation 428/2009 and for Cyber-Surveillance Controls Promoting Human Rights and International Humanitarian Law Globally. 2018, WK 5755/2018 INIT.
47 DIGITAL EUROPE. Updated DIGITAL EUROPE comments on proposal for recast of export control regulation. [online]. 2018. Dostupné na <https://www.digitaleurope.org/resources/updated-digitaleurope-comments-on-proposal-for-recast-of-export-control-regulation/>.
48 Bundesverband der Deutschen Industrie. EC dual-use: review of the EC dual-use regulation. [online]. 2016. Dostupné na <https://bdi.eu/media/topics/global_issues/downloads/201601_FINAL_BDI-Assessment_Reform_EC_Dual-Use.pdf>.
49 Pro kritiku tohoto přístup viz RIECKE, L. Unmasking the Term ‚Dual Use' in EU Spyware Export Control. *European Journal of International Law*, 2023, sv. 34, č. 3, str. 697–720.
50 GREGOROVÁ, M. The European Parliament's expectations for more effective controls on cybersurveillance technologies. In: *2020 Export Control Forum* [online]. 2020. Dostupné na <https://trade.ec.europa.eu/doclib/docs/2020/december/tradoc_159190.pdf>.
51 Evropská komise představila první návrh za slovenského předsednictví v září 2016. Následně diskuze probíhaly za předsednictví Malty, Estonska, Bulharska, Rakouska, Rumunska a Finska, než se podařilo dosáhnout dohody na předložení návrhu Evropskému parlamentu, se kterým vyjednávalo o konečné verzi chorvatské a poté německé předsednictví v druhé polovině r. 2020.
52 Viz také SVOBODA, O. Úloha Evropského parlamentu při prosazování lidských práv v obchodní politice. *Acta Universitatis Carolinae* Iuridica, 2021, sv. 67, č. 1.

významně ovlivnit vývoj v této oblasti na globální úrovni. Může totiž představovat krok směrem k překonání chybějících jasných pravidel pro technologie dohledu a jejich použití v kyberprostoru. Není náhodou, že kontrola vývozu je také jedním z nosných témat Rady pro obchod a technologie (TTC) založené EU a USA jako součást „nové transatlantické agendy pro celosvětovou změnu".[53] Mezi hlavní aktivity TTC patří nalezení společného přístupu k ochraně kritických technologií, vč. kontroly vývozu, stejně jako spolupráce na jejich pravidlech a standardech.[54] Taková spolupráce v případě EU i USA jako u podobně smýšlejících partnerů dává smysl a mělo by se to projevit typicky v koordinaci legislativních iniciativ nebo společného přístupu v mezinárodních organizacích vyvíjející nové standardy.

Kontury nového regulačního rámce ve světle náležité péče

Obecné zásady OSN nabízejí pro celou šíři podniků „bez ohledu na jejich velikost, odvětví, prostředí, ve kterém působí, vlastnictví a strukturu"[55] komplexní rámec k zabránění nepříznivého dopadu na lidská práva a také jeho předcházení a zmírňování v důsledku digitálních technologií. Ve stejném roce, kdy Rada OSN pro lidská práva přijala tyto zásady, Směrnice OECD pro nadnárodní podniky převzala dva významné prvky: důležitost náležité péče ve vnitrofiremních postupech při nesení odpovědnosti za dodržování lidských práv a požadavek náležité péče na všechny subjekty zahrnuté ve Směrnici OECD.[56]

Společně tyto dva dokumenty vyvářejí rámec založený na zásadách náležité péče, transparentnosti, odpovědnosti a nápravy, který by měl omezovat negativní lidskoprávní dopady. Ačkoliv se jedná o nezávazné mezinárodní standardy *(soft law)*,[57] vedou ke vzniku prostředí, ve kterém se od byznysu v rostoucí míře očekává, že bude zohledňovat faktor ochrany lidských práv ve všech obchodních aktivitách. Tímto způsobem také nabízejí návod pro společnosti v sektoru ICT, jak by se měly chovat a zmírňovat negativní dopady jejich sledovacích technologií. Je třeba však podotknout, že uvádění těchto standardů do praxe je pomalé. Důvod je zřejmý, a to již zmiňovaná nezávaznost.

Tento stav nekompenzuje ani existence implementačního mechanismu pro Směrnici OECD: sítě Národních kontaktních míst (NKM), které jsou zřízeny v každém státu, který ke Směrnici OECD přistoupil.[58] Příkladem této inherentní slabiny je případ britské společnosti Gamma Group. Její dceřiná společnost FinFisher a její německý partner, společnost Trovicor, prodávaly sledovací technologie bahrajnské vládě. Poté, co se tato informace dostala na veřejnost, několik nevládních organizací podalo stížnosti u NKM ve Velké Británii a Německu proti uvedeným společnostem. Zatímco německé NKM stížnost proti Trovicoru odmítlo kvůli nedostatku důkazů, britské NKM stížnost proti Gamma Group přijalo. Následně ve svém úvodním posouzení konstatovalo, že „i když ani jedna ze stran nenabídla přímý důkaz o dodávkách Gammy do Bahrajnu, důkazy nasvědčují tomu, že produkt společnosti mohl být používán proti bahrajnským aktivistům. NKM se domnívalo, že to otevírá otázky ohledně povinnosti společnosti provádět náležitou péči a zabývat se možnými dopady."[59] V konečném posouzení NKM uzavřelo, že Gamma porušila Směrnici OECD, a vydalo několik doporučení, především k posílení transparentnosti, v jejích obchodních operacích a poskytování nápravy při zneužití jejích produktů.[60] Následná zpráva NKM hodnotící navazující kroky ze strany společnosti bohužel konstatovala, že „při absenci informací od Gammy může NKM Velké Británie pouze uzavřít, že Gamma International UK Limited neučinila vůbec žádný pokrok (ani úsilí)" a „nevidíme tak žádný důvod ke změně názoru, ke kterému se dospělo v konečném posouzení, že chování Gammy

53 Evropská komise. EU-USA: Nová transatlantická agenda pro globální změny. 2. 12. 2020.

54 Pro srovnání evropského a amerického přístupu v oblasti kontroly vývozu zboží dvojího užití viz KANETAKE, M. Dual-Use Export Control: Security and Human Rights Challenges to Multilateralism. In: Bungenberg, M. – Krajewski, M. – Tams, C. J. – Terhechte, J. P. – Ziegler, A.R. (eds). *European Yearbook of International Economic Law 2020*, Cham 2021, str. 265–290; WHANG, C. Trade and Emerging Technologies: A Comparative Analysis of the United States and the European Union Dual-Use Export Control Regulations. *Security and Human Rights*, 2021, sv. 31, str. 11–34.

55 Obecné zásady OSN v oblasti podnikání a lidských práv, zásada 14.

56 RUGGIE, J. G. – NELSON, T. Human rights and the OECD guidelines for multinational enterprises: normative innovations and implementation challenges. *Brown Journal of World Affairs*, 2015, sv. 22, č. 1, str. 170–171.

57 Ke konceptu *soft law* viz blíže např. HUBKOVÁ, P. Mezinárodní soft law jako koncept v judikatuře správních soudů. *Jurisprudence*, 2022, č. 5, str. 1–3.

58 SVOBODA O. The OECD guidelines for multinational enterprises and the increasing relevance of the system of National Contact Points. In: Šturma P. – Mozetic, V. A. (eds.). *Business and Human Rights*, Waldkirchen 2018, str. 50.

59 UK National Contact Point. *Initial assessment: Privacy International complaint to UK NCP about Gamma International UK Ltd*. 2013, odst. 25.

60 UK National Contact Point, *Privacy International & Gamma International UK Ltd.: final statement after examination of complaint*. 2014, odst. 68–69.

není v souladu se závazky obsaženými ve Směrnici OECD".[61]

Oba případy tak nabízí příklad toho, jakým překážkám síť NKM čelí při prosazování odpovědného obchodního chování firem (nejen) v odvětví ICT. Ilustrují také, jak je obtížné v rámci nezávazných standardů vynucovat dodržování ochrany lidských práv mezi vývozci technologií kybernetického dohledu. Není proto ani příliš překvapivé, že pro některé nevládní organizace případy projednávané před NKM spíše dokazují neschopnost tohoto mechanismu poskytnout účinnou nápravu v situacích, kdy dochází k porušování lidských práv v souvislosti s prodejem sledovacích technologií.[62]

Navzdory odůvodněnému skepticismu lze ale také na druhou stranu najít příklady, kdy kritizované společnosti zaujaly kooperativní postoj. V červnu 2020 podala švýcarská nevládní organizace Society for Threatened Peoples stížnost ke švýcarskému NKM na obchodní operace banky UBS (Union Bank of Switzerland) Group s čínskou společností Hikvision, která je největším výrobce a vývojářem sledovacích technologií na světě. Hraje proto také důležitou roli v provincii Sin-ťiang, kvůli které se dostala v říjnu 2019 na černý seznam americké vlády pro porušování lidských práv.[63] Podle Society for Threatened Peoples skupina USB tím, že udržovala finanční vazby s touto společností, porušovala nejen vlastní kodex chování, ale také Směrnici OECD. Ačkoliv USB toto obvinění odmítla, vedla se Society for Threatened Peoples strukturovaný a kontinuální dialog v rámci mediace poskytnuté švýcarským NKM. To případ uzavřelo konstatováním, že USB souhlasilo s převzetím vedoucí role ve finančním průmyslu při upozorňování na ESG kritéria, vč. zohledňování lidských práv, v kontextu pasivních investičních fondů a pokračováním diskuzí s nevládním sektorem, jak dále podpořit ochranu lidských práv.[64]

Schopnost sítě NKM OECD poskytovat účinnou nápravu zůstává ale omezená, nekonzistentní a nepředvídatelná.[65] Přesto ale dosahuje navzdory své právní povaze a struktuře řady pozitivních výsledků. Při kontinuálním zlepšování a ve spojení s dalšími nástroji může mít také velmi pozitivní vliv na „lidskoprávní kultivaci" vývozu technologií. Zvláště nadějné to může být v kontextu lidskoprávní náležité péče a procesů vnitřní kontroly sloužících identifikaci a zmírnění dopadů podniku na lidská práva či k jejich předcházení a ke stanovení odpovědnosti za řešení těchto dopadů.[66]

Mezinárodní standardy a soukromá seberegulace

Zapracování lidskoprávních zásad ze strany společností v ICT sektoru a při jejich obchodních operacích nebylo dosud příliš významné.[67] Taková je realita navzdory tomu, že Obecné zásady OSN představují „celosvětový standard očekávaného chování" ze strany všech společností při jejich obchodních aktivitách.[68] Mělo by být navíc zřejmé, že stanovují pouze nejnižší úroveň při posuzování, zda společnost při vývozu jejích produktů a služeb zohledňuje lidskoprávní dopady. Státy by v tomto směru měly být aktivnější při prosazování nových standardů, které mohou mít zásadní roli při zavádění odpovědného vývozu sledovacích technologií. Konkrétně mohou vlády vést debatu nad účinnější prevencí a dovést soukromé subjekty k formulaci vlastních standardů.

V tomto směru již existují i konkrétní první příklady, např. *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*, kterou připravila Evropská komise ve spolupráci s Institutem pro lidská práva a byznys,[69] příručka *Know Your Customer Standards for Sales of Surveillance Equipment* připravená Electric Frontiers Foundations[70] nebo soubor vodítek o zamezování hrozeb spojených s vývozem a použitím kyberbezpečnostních systémů, který publikovala

61 UK National Contact Point. *Follow-up statement: Privacy International complaint to UK NCP about Gamma International*. 2016, odst. 9.
62 International Federation for Human Rights. *Surveillance technologies "Made in Europe": regulation needed to prevent human rights abuses*. 2014, str. 26–27.
63 US Department of Commerce. Addition of Certain Entities to the Entity List. *Federal Register*, Vol. 84, No. 196, 9. 10. 2019.
64 National Contact Point of Switzerland. *National Contact Point of Switzerland Final Statement. Specific Instance regarding UBS Group AG submitted by the Society for Threatened Peoples Switzerland*. 12. 12. 2021, str. 1.
65 BHATT, K. – ERDEM TURKELLLI, G. OECD National Contact Points as Sites of Effective Remedy: New Expressions of the Role and Rule of Law within Market Globalization. *Business and Human Rights Journal*, 2021, sv. 6, č. 3, str. 447.
66 K tomuto cíli směřuje i aktivita OECD, kdy v posledních několika letech přijala Vodítka pro náležitou péči a sektorové pokyny (Pokyny pro odpovědné obchodní řetězce v textilním a obuvnickém odvětví; Pokyny OECD-FAO pro odpovědné zemědělské dodavatelské řetězce; Pokyny pro odpovědné obchodní jednání institucionálních investorů; Pokyny OECD pro náležitou péči v odpovědných dodavatelských řetězcích nerostných surovin z oblastí postižených konflikty a vysoce rizikových oblastí).
67 Human Rights Council. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. 2015, UN DOC A/HRC/29/32, odst. 10.
68 Obecné zásady OSN v oblasti podnikání a lidských práv, zásada 11: Podniky by měly respektovat lidská práva. Měly by se tedy vyvarovat porušování lidských práv, a dochází-li v souvislosti s nimi k nepříznivému vlivu na lidská práva, měly by se jím zabývat.
69 European Commission. *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. 2014.
70 COHN C., YORK J. C. "Know Your Customer" standards for sales of surveillance equipment. In: *Electric Frontiers Foundations* [online]. 24. 10. 2011. Dostupné na <https://www.eff.org/deeplinks/2011/10/its-time-know-your-customer-standards-sales-surveillance-equipment>.

britská oborová asociace TechUK a byla v této činnosti podpořena britskou vládou.[71]

Nejnovější významnou státy iniciovanou aktivitou je *Export Controls and Human Rights Initiative*, která byla oznámena na Summitu pro demokracii v prosinci 2021.[72] O více než dva roky později se rozšířila z 8 na 25 států, jež se v březnu 2023 přihlásily ke kodexu chování posilujícího kontroly vývozu zboží a technologií, které mohou být zneužity a vést k závažnému porušování lidských práv. Zapojené státy se mj. přihlásily ke konzultacím a podpoře soukromého sektoru v implementaci postupů náležité péče v souladu s vnitrostátním právem a Obecnými zásadami OSN. Za pozornost také stojí, že státy se zavázaly ke spolupráci v rámci mnohostranných kontrolních režimů a souvisejících iniciativ.[73]

Navzdory těmto snahám veřejně dostupné informace příliš nenasvědčují tomu, že lidskoprávní náležitá péče je běžnou součástí prodeje a následného servisu při exportu technologií. Tento pocit je dále umocněn důkazy o tom, jak řada technologických společností v Evropě či Americe přispívala a stále přispívá k porušování lidských práv v zahraničí, často skrytě při nedostatečné transparentnosti a mlčení o firemních pojistkách, který by tomu měli bránit. Pro některé experty je právě nedostatečné informování ze strany společností potvrzením toho, že jejich interní standardy nemají reálnou přidanou hodnotu a že nezavádí v dostatečné míře opatření k posílení náležité péče, transparentnosti a odpovědnosti.[74] Takové závěry jistě nevrhají pozitivní světlo na celé odvětví ICT a jeho ochotu přijmout odpovědné obchodní politiky. Je tedy stále potřebná aktivnější role státu, která povede k zavedení náležité péče k nalezení, zabránění a zmírnění škodlivých lidskoprávních dopadů stejně jako ke kompenzačním mechanismům pro poškozené držitele těchto práv.[75]

Pořád však také platí, že velkou část práce spojenou se zavedením nových standardů může odvést samotný průmysl ve standardizačních organizacích nebo platformách sdružujících různé zájmové skupiny, jako např. Global Network Initiative.[76] Na jejich půdě se mohou definovat osvědčené postupy náležité péče v odvětví ICT. Tento přístup může mít i další výhody. První je zapojení širší skupiny subjektů, které se diskuzí v těchto formátech účastní. Druhým pozitivem je vyšší transparentnost při vytváření a přijímání pravidel v takovém prostředí.

Specializované používání informačních a telekomunikačních technologií je oblastí, ve které průmysl a technologické společnosti mohou hrát ústřední roli při vydávání oborově zaměřených doporučení při zohlednění Obecných zásad OSN, Směrnice OECD a uplatňování náležité péče. Zvláštní pozornost by měla být věnována tomu, aby se jednalo o „chytrou" regulaci, která bude flexibilní, efektivní a komplexní, přičemž náležitá péče by měla být jedním z jejich hlavních pilířů.[77] Aby byly iniciativy průmyslu brány vážně a měly i praktický dopad, je v první řadě nutné, aby ve svých vývozních aktivitách dodržovaly zásady odpovědného obchodního chování.

Je např. typické, že spolupráce mezi vývozcem technologie a kupující státní institucí nekončí momentem prodeje a technologickým transferem. Uniklé dokumenty potvrzují, že společnosti obvykle následně poskytují služby *after care*, které mohou trvat i několik let po samotné transakci, např. ve formě balíčku metod technologie sledování a odposlechu, jakož i výcvik pro zaměstnance a technickou, provozní a metodickou podporu.[78] Proto je důležité, aby společnosti z ICT odvětví uplatňovaly náležitou péči nejen před prodejem, ale i poté. Zároveň by společnosti měly mít zabudované interní mechanismy kontroly a nápravy, protože kombinace kyberprostoru a rostoucího množství digitálních informací zvyšuje šanci k jejich zneužití.[79] Na takové situace by měli být vývozci citlivých technologií kybernetického dohledu připraveni.

---

71 TechUK. *Assessing cyber security export risks*. [online]. 2014. Dostupné na <https://www.computerweekly.com/news/2240235381/TechUK-publishes-guidelines-for-UK-cyber-security-exports>.

72 White House. Joint Statement on the Export Controls and Human Rights Initiative. 10. 12. 2021.

73 Department of State. *Code of Conduct for Enhancing Export Controls of Goods and Technology That Could be Misused and Lead to Serious Violations or Abuses of Human Rights*. 30. 3. 2023.

74 Human Rights Council. *Surveillance and human rights: report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. 2019, A/HRC/41/35, odst. 32.

75 Human Rights Council. *Report of the Special Representative of the Secretary General on the issue of human rights and transnational corporations and other business enterprises*. 2011, UN DOC A/HRC/17/31, odst. 15–25.

76 MAURER, T. Internet freedom and export controls. In: *Carnegie Endowment* [online]. 3. 3. 2016. Dostupné na <https://carnegieendowment.org/2016/03/03/internet-freedom-and-export-controls-pub-62961>.

77 Viz také Global Conference on Cyberspace 2015. Chair's Statement. In: *MOFA* [online]. 17. 4. 2015. Dostupné na <https://www.mofa.go.jp/mofaj/files/000076862.pdf>.

78 Privacy International. Six things we know from the latest FinFisher documents. [online]. 15. 8. 2014. Dostupné na <https://privacyinternational.org/blog/1522/six-things-we-know-latest-finfisher-documents>. Viz také Doporučení Evropského parlamentu ze dne 15. června 2023 Radě a Komisi v návaznosti na vyšetřování údajných porušení a správních pochybení v oblasti provádění právních předpisů Unie týkajících se používání špionážního softwaru Pegasus a ekvivalentního špionážního softwaru (2023/2500(RSP)), 15. 6. 2023, odst. AR.

79 LIPOVSKÝ, M. Digital aspects of the right to privacy – surveillance issues. *Czech Yearbook of Public Private International Law*, 2016, sv. 7, str. 264.

Závěr

V posledních letech jsme svědky posilujícího a znepokojivého trendu, kdy státy, především ty ovládané autoritativními režimy, v rostoucí míře využívají nejmodernějších technologií kybernetického dohledu. Tyto technologie usnadňují zásahy do soukromí člověka, kdy umožňují sledování osob a zaznamenávání jejich chování, ať už na veřejnosti, nebo v soukromí. Informační společnost bude přinášet nové a nové technologie zasahující do soukromí lidí a lze konstatovat, že schopnost celospolečenské kontroly a jejího zneužívání dosahuje díky novým technologiím již nyní bezprecedentní úrovně. Netransparentní postupy států i technologických společností při sběru osobních údajů nebo zavádění technologií rozpoznávajících tváře vážně ohrožují soukromí a svobodu jednotlivců. Efektivní ochrana před svévolnými zásahy do soukromí jednotlivců v kybernetickém prostoru je přitom nutným předpokladem pro uplatňování dalších lidských práv, včetně práva na svobodu projevu a práva na pokojné shromažďování.

Popisovaná dynamika v oblasti kybernetické bezpečnosti a technologií se bude dále rozvíjet a rostoucí propojení problematiky technologického pokroku a hospodářského rozvoje na jedné straně a lidských práv na straně druhé je nevyhnutelné. Do této roviny však vstupuje ještě třetí oblast, a to kontrola vývozu. To zřetelně dokládá vývoj poslední úpravy kontroly vývozu v EU, který byl v první řadě motivován lidskoprávními úvahami. Vzniká tak triangulární vztah, který byl předmětem tohoto příspěvku.

K zajištění účinné a systematické kontroly vývozu zneužitelných technologií do nedemokratických zemí je však potřeba nastavit pravidla, která se nebudou spoléhat pouze na přísnou kontrolu vývozu státními orgány. Je nutné, aby obchodní a technologické společnosti přijaly za své zásady náležité péče, které jsou v souladu s širšími principy Obecných zásad OSN a Směrnice OECD. K podobné vizi se nedávno přihlásila i Rada EU, kdy vyzvala k „nalezení společného základu a sladěných strategických vizí založených na sdílených hodnotách a zájmech v průsečíku technologického rozvoje, normalizace a geopolitiky, které budou prospěšné jak pro EU, tak pro průmysl“.[80] V rostoucí míře se dá v této oblasti spoléhat na síť NKM OECD. Souběžně je také třeba důsledně a systematicky vést průmysl k odpovědnosti a vytvoření a dodržování vlastních standardů náležité péče.

V každém případě se zdá, že prolínání regulace vývozu (i dovozu) s ochranou lidských práv se zintenzivňuje. V lednu 2024 Komise přijala pět iniciativ k posílení hospodářské bezpečnosti EU v době rostoucího geopolitického napětí a hlubokých technologických změn. Jednou z nich je Bílá kniha ke kontrolám vývozu, kde Komise upozorňuje na potřebu zefektivnění systému kontrol a větší evropské koordinace u vývozu technologií dvojího užití s ohledem na jejich dynamický vývoj a tak, aby toto zboží nebylo využíváno k oslabování bezpečnosti a lidských práv.[81] V březnu 2024 se pak podařilo dosáhnout kompromisu mezi evropskými institucemi nad návrhem směrnice o náležité péči podniků v oblasti udržitelnosti, která zavede povinnost náležité péče podniků v oblasti udržitelnosti s cílem řešit negativní dopady na lidská práva a životní prostředí.

[80] Rada EU. Závěry Rady o digitální diplomacii EU – závěry Rady schválené Radou na zasedání dne 26. 6. 2023, odst. 14.
[81] Evropská komise. Bílá kniha o kontrolách vývozu. COM(2024) 25 final, 24. 1. 2024.