Cybernetyka, bezpieczeństwo, prywatność

Polska Akademia Nauk
Oddział w Poznaniu

Cybernetyka, bezpieczeństwo, prywatność

Artykuły opracowane na podstawie referatów wygłoszonych podczas XXI sesji naukowej z cyklu „Dwugłos Nauki" w Poznaniu, 28 listopada 2019 roku

Pod redakcją
prof. dr. hab. Marka Świtońskiego

Poznań 2020

Polska Akademia Nauk, Oddział w Poznaniu
Cybernetyka, bezpieczeństwo, prywatność

Publikacja finansowana przez
Polską Akademię Nauk

ISBN 978-83-63305-86-4

Projekt okładki: Mirosława Korbańska
Korekta: Małgorzata Szkudlarska

Polska Akademia Nauk, Oddział w Poznaniu
61-772 Poznań, Stary Rynek 78/79
tel.: (61) 641 50 03
e-mail: poznan@pan.pl, poznan.pan.pl

Przygotowanie do druku:
Logoscript Sp. z o.o.
ul. Dembowskiego 5/54
02-784 Warszawa

Druk i oprawa:
Agencja Wydawniczo-Poligraficzna GIMPO
ul. Transportowców 11, 02-858 Warszawa
tel. +48 501 076 031
e-mail: gimpo@poligrafia.waw.pl

SPIS TREŚCI

WPROWADZENIE

XXI edycja seminarium naukowego z cyklu „Dwugłos Nauki", której organizatorami są Oddział Polskiej Akademii Nauk w Poznaniu i Wydział Teologiczny Uniwersytetu im. Adama Mickiewicza w Poznaniu, odbyła się 28 listopada 2019 roku w Pałacu Działyńskich, w siedzibie Oddziału PAN w Poznaniu. Tematem przewodnim sesji, której tytuł brzmiał *Cybernetyka. Bezpieczeństwo. Prywatność*, była pozycja człowieka w cyberprzestrzeni, definiowanej jako przestrzeń komunikacyjna tworzona przez systemy powiązań internetowych, która pozwala na komunikowanie się w sieci i nawiązywanie relacji w czasie rzeczywistym (M. Marczyk, 2018, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny" nr 1-2, s. 59-72). W ramach sesji wygłoszono cztery referaty. Dwa z nich był poświęcone technologiom cybernetycznym, a dwa konsekwencjom filozoficzno-socjologicznym obserwowanym we współczesnych społeczeństwach. W niniejszej książce zaprezentowane są teksty nawiązujące do wygłoszonych referatów.

Cybernetyka, czyli nauka o sterowaniu oraz przesyłaniu i przetwarzaniu informacji w systemach technicznych, biologicznych i społecznych (wg PWN), rozwija się niezwykle dynamicznie. Blisko 30 lat temu, było to w 1991 roku, Internet stał się w Polsce oficjalnie dostępny. Możliwość korzystania z poczty elektronicznej niezwykle przyspieszyła tempo komunikowana się między użytkownikami, a swobodny dostęp do baz danych sprawił, że uzyskanie poszukiwanych informacji stało się łatwe. Dodatkowo rozwój telefonii komórkowej sprawił, że nieomal każdy z nas ma przy sobie urządzenie (smartfon), które nie tylko umożliwia komunikowanie się głosowe, wizyjne czy tekstowe, ale również łączenie się z ogólnoświatową siecią internetową. Do tego doszły serwisy społecznościowe (Facebook, Instagram, Twitter), które sprawiły, że możemy na bieżąco śledzić losy użytkowników tych serwisów, którzy zdecydowali się na taką formę autoprezentacji (zdjęcia z wakacji, zdarzenia z życia rodzinnego, wyrażanie poglądów, opinii itp.).

Ponadto powszechny stał się marketing internetowy. Trudno sobie wyobrazić codzienne funkcjonowanie bez dostępu do informacji „tu i teraz". Siedzimy przy komputerze lub sięgamy do kieszeni po smartfona i w ciągu kilkunastu sekund możemy dotrzeć do wybranego artykułu naukowego, bazy danych, najnowszych informacji politycznych, sportowych, kulturalnych, wytyczyć drogę do wybranego celu lub kupić lodówkę, buty czy inny produkt. Ale ten luksus ma swoją cenę, której niejednokrotnie wolelibyśmy uniknąć.

Ogromne możliwości współczesnych komputerów oraz specjalistyczne oprogramowania powiązane z siecią internetową umożliwiają śledzenie nieomal każdego naszego kroku dzięki kamerom na skrzyżowaniach ulic, w tramwajach, pociągach, na lotniskach, w samochodach, na kaskach motocyklistów. Analizy socjologiczne i psychologiczne pozwalają na przygotowanie spersonalizowanych informacji wysyłanych do użytkowników mediów społecznościowych w celu wpływu na ich decyzje, także wyborcze. Co więcej, wyrafinowane oprogramowania pozwalają na „infekowanie" telefonów komórkowych, bez wiedzy użytkownika, w celu kontrolowania i przetwarzania treści wiadomości przesyłanych w mailach czy SMS-ach. Nieco ponad 20 lat temu (1998) trafił na ekrany kin film pt. *Truman show*, w którym życie głównego bohatera było śledzone (bez jego wiedzy) od narodzin przez kilka tysięcy ukrytych kamer, a wszyscy ludzie wokół niego to aktorzy, którzy sterują jego życiem. Co więcej, nagrania z życia są emitowane w formie serialu telewizyjnego. Film ten można dzisiaj traktować jako zwiastun współczesnej pozycji człowieka w cyberprzestrzeni. A przecież ta najbliższa i nieco dalsza przyszłość przyniesie kolejne osiągnięcia technologiczne. Czy jesteśmy na nie przygotowani? Czy aktualna cyberprzestrzeń czyni nas wolniejszymi, bezpieczniejszymi, szczęśliwszymi?

Pozycja człowieka w cyberprzestrzeni, w wymiarze socjologicznym, psychologicznym, etycznym, filozoficznym czy prawnym, to zagadnienia bardzo aktualne i ważne. Publikowane są podręczniki akademickie (np. M.R. Jabłońska, 2018, *Człowiek w cyberprzestrzeni. Wprowadzenie do psychologii Internetu*, Wydawnictwo Uniwersytetu Łódzkiego) oraz uruchomiane są kierunki studiów (np. człowiek w cyberprzestrzeni, studia I stopnia na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie) poświęcone temu zagadnieniu.

Mam nadzieję, że lektura kolejnych rozdziałów niniejszej książki uświadomi nam możliwości współczesnej cybernetyki oraz konsekwencje wynikające z tego dla człowieka. Dwa spośród tych rozdziałów skoncentrowane są na postępie technologicznym cybernetyki, a kolejne

dwa na jego kontekście filozoficznym i socjologicznym. Autorami rozdziałów w niniejszej książce są prelegenci XXI sesji „Dwugłos Nauki":

- prof. dr hab. Krzysztof Stachewicz z Uniwersytetu im. A. Mickiewicza w Poznaniu,
- prof. UMK dr hab. Radosław Sojak z Uniwersytetu Mikołaja Kopernika w Toruniu,
- dr inż. Maciej Miłostan oraz dr inż. Michał Szychowiak z Politechniki Poznańskiej.

PT Prelegentom wyrażam gorące podziękowanie za przyjęcie zaproszenia do udziału w seminarium oraz przygotowanie tekstów wygłoszonych referatów. Pragnę także podziękować Panu prof. dr. hab. inż. Romanowi Słowińskiemu, czł. rzecz. PAN, oraz o. prof. UAM dr. hab. Sergiuszowi Nizińskiemu OCD za przewodniczenie sesjom i prowadzenie dyskusji.

Prof. dr hab. Marek Świtoński, czł. koresp. PAN
Prezes Oddziału Polskiej Akademii Nauk w Poznaniu

NOWE TECHNOLOGIE I MY. GDZIE SIĘ PODZIAŁA NASZA PRYWATNOŚĆ?

MICHAŁ SZYCHOWIAK

Politechnika Poznańska

Niewątpliwie żyjemy dziś w świecie permanentnej inwigilacji, w którym nieustannie, zachłannie i coraz bardziej inwazyjnie pozyskuje się i gromadzi nasze prywatne dane. Szacuje się, że w 2020 roku ich rozmiar sięgnie dziesiątek zettabajtów (tryliardów bajtów)[1]. Lwia część tych informacji pochodzi z naszej świadomej codziennej aktywności w sieci (wg szacunków przeciętny użytkownik Internetu poświęca mu ponad 2 godziny dziennie[2]), ale coraz większy udział w pozyskiwaniu danych mają inne nowoczesne technologie, natarczywie zdobywające kolejne segmenty rynku. Zarówno najprostsze, jak i te najwymyślniejsze gadżety elektroniczne są dziś wyposażane w mechanizmy komunikacji bezprzewodowej, umożliwiające im dostęp do naszych sieci domowych i dalej do Internetu. W ciągu ostatnich 10 lat powstała i rozpowszechniła się niezliczona wręcz ilość technologii komunikacyjnych, protokołów, funkcji i usług, stworzonych – według zapewnień twórców – by oferować nam jak największą wygodę korzystania z dobrodziejstw wirtualnego świata. A kolejne wynalazki już ustawiają się w kolejce po swój kawałek rynku. Tylko czy aby na pewno jedynym celem ich istnienia jest przemożna chęć uczynienia naszego życia łatwiejszym i wygodniejszym?

[1] N. Patrignani, D. Whitehouse, Monica Gemo, „Forget About Privacy… or Not?", IFIP AICT 526, pp. 76–85, 2018

[2] „Average Time Spent per Day with Mobile Internet" www.emarketer.com

Czy część rynku nowych technologii przypadkiem nie celuje z premedytacją w pozyskiwanie bodaj najcenniejszego dziś surowca naturalnego naszej planety – informacji?

Informacje o nas, naszych zainteresowaniach, przyzwyczajeniach, preferencjach, które mniej czy bardziej świadomie pozostawiamy po swojej aktywności m.in. w serwisach społecznościowych, na forach dyskusyjnych, przeróżnych blogach, vlogach itp., stanowią prawdziwą żyłę złota dla agencji reklamowych i marketingowych, oraz wielu innych rodzajów firm potrzebujących ich do podejmowania decyzji biznesowych. Informacje te są dostępne niemal na wyciągnięcie ręki i to na ogół kompletnie za darmo. Nic dziwnego, że wielu zainteresowanych nie potrafi oprzeć się pokusie, opracowując coraz to bardziej wyrafinowane sposoby pozyskiwania naszych prywatnych danych.

Dzieje się aktualnie w tej materii dużo, i to, niestety, dużo złego. Na tyle dużo, że coraz więcej instytucji rządowych[3] i organizacji społecznych[4] zainteresowanych bezpieczeństwem i prywatnością obywateli bije na alarm.

Za część zagrożeń prywatności odpowiadają służby i agencje rządowe[5]. Przykładowo Chiny rozpoczęły właśnie budowę krajowego systemu oceniającego swoich obywateli (*China Social Credit System*), w ramach którego na indywidualnym koncie każdego obywatela ChRL gromadzone są swoistego rodzaju punkty (przypominające w swej istocie punkty karne przyznawane w wielu krajach za wykroczenia drogowe), będące podstawą indywidualnej oceny obywatela i ewentualnych przyszłych decyzji administracyjnych w odniesieniu do jego osoby. Tej punktacji podlega dość pokaźny zbiór codziennych aktywności – od nawyków zakupowych począwszy, na aktywności społecznej skończywszy[6].

---

[3] Przykładowo w Stanach Zjednoczonych: D. Solove, W. Hartzog, „The FTC and the new common law of privacy", Columbia Law Rev. 114(3), 583–676 (2014), https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement; oraz w Unii Europejskiej: Parliamentary Assembly of the Council of Europe, Committee on Legal Affairs and Human Rights, „Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", ETS No. 108 + Report 14437, 2017.

[4] K. Szymielewicz, K. Iwańska, „Śledzenie i profilowanie w sieci", Raport fundacji Panoptykon, 2019, https://panoptykon.org/sites/default/files/publikacje/panoptykon_raport_o_sledzeniu_final.pdf; patrz też: https://panoptykon.org/zapleczeinternetu.

[5] Przykładowo: https://www.tvn24.pl/system-pegasus-i-pytania-do-cba-czarno-na-bialym,964972,s.html.

[6] R. Botsman, „Big data meets Big Brother as China moves to rate its citizens", Wired, https://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion, 2017.

Paradoksalnie, dużo większą skalę osiągnął jednak międzynarodowy proceder pozyskiwania danych pojawiających się w sieci przy udziale samego użytkownika, rozwinięty przez serwisy internetowe (media społecznościowe, sklepy internetowe, instytucje finansowe i kredytowe itp.) i aplikacje mobilne instalowane we wszechobecnych telefonach komórkowych[7]. Dane pozyskiwane z tych źródeł są zbierane przez wyspecjalizowane firmy z sektora prywatnego – brokerów danych (zwykle o międzynarodowym zasięgu) i wykorzystywane do profilowania konsumentów, by ostatecznie zostać odsprzedanymi dalej za jak najwyższą cenę na elektronicznych giełdach danych osobowych.

Niektóre skutecznie wylansowane wśród młodzieży (i nie tylko) gry mobilne, całkowicie darmowe – oczywiście – nie służą praktycznie niczemu innemu jak tylko śledzeniu użytkownika, czego świadomość wśród tych ostatnich jest jeszcze cały czas niedostateczna[8].

Niebezpieczeństwo potencjalnie największej skali mogą skrywać zyskujące popularność wśród konsumentów na całym świecie różnorodne elektroniczne gadżety, określane wspólnym mianem Internetu Rzeczy lub Internetu Przedmiotów (ang. *Internet of Things*, IoT[9]). To bardzo pojemna kategoria urządzeń, obejmująca m.in. domowe urządzenia sieciowe (routery dostępowe, koncentratory IoT i in.), telewizory SmartTV, kamery monitorujące, inteligentne termostaty, mierniki energii i mediów, żarówki, ekspresy do kawy, lodówki i jeszcze wiele, wiele innych przedziwnych pomysłów naszpikowania przedmiotów codziennego użytku elektroniką, skądinąd zupełnie zbyteczną do ich normalnej pracy. Bardzo reprezentatywnym tego przykładem są chociażby „inteligentne" materace do łóżek, wymagające teraz elektrycznego zasilania (a jakże!), by móc świadczyć swoje „inteligentne" usługi użytkownikowi. Użytkownikowi, no i – rzecz jasna – producentowi, który zapewne chętnie odsprzeda wszelkie pozyskane informacje dalej, np. brokerom danych, najchętniej po cichu, na ile się tylko da, bez zbytecznego kłopotania użytkownika tym faktem. I na ile akurat pozwoli mu obowiązujące prawo (szczęśliwie dla konsumentów Unia Europejska narzuca tu pewne ograniczenia wynikające z RODO[10], jednak istotną trudnością okazuje się

[7] S. Kununka, N. Mehandjiev, P. Sampaio, „A Comparative Study of Android and iOS Mobile Applications' Data Handling Practices Versus Compliance to Privacy Policy", IFIP AICT 526, pp. 301–313, 2018.

[8] D. Harborth, S. Pape, „Privacy Concerns and Behavior of Pokémon G. Players in Germany", IFIP AICT 526, pp. 314–329, 2018.

[9] J.H. Ziegeldorf et al., „Privacy in the Internet of Things: threats and challenges", Secur. Commun. Netw. 7, pp. 2728–2742, 2014.

[10] General Data Protection Regulation 2016/679/EU, http://eugdpr.org.

fakt, iż zasady prawne określane w uchwalanych przepisach zwykle nie poddają się łatwemu przełożeniu na rozwiązania technologiczne mające szanse sprawdzić się w praktyce[11]).

Tak czy inaczej, nagminne okazują się być przeróżne formy pozyskiwania prywatnych informacji przez urządzenia IoT[12]. Obszerne analizy rynku urządzeń IoT pod względem prywatności danych można znaleźć m.in. w wielu materiałach konferencyjnych[13].

Ogromna liczba oferowanych na tym rynku produktów niesie zagrożenie nie tylko dla naszej prywatności, ale i szerzej rozumianego bezpieczeństwa[14] (w tym kontekście coraz więcej krajów zaczyna niepokoić fakt, iż zdecydowana większość komponentów rynku elektronicznego jest produkowana w Państwie Środka). Od co najmniej 2014 roku znane są przypadki przejmowania przez hakerów kontroli nad tragicznie słabo zabezpieczonymi urządzeniami domowymi (nawet rzędu 100 tys. urządzeń jednorazowo[15]) i wykorzystywania ich – całkowicie bez świadomości właścicieli – do różnego rodzaju nielegalnego procederu, np. rozsyłania pocztowego spamu. Zagrożenia nie omijają nawet tak pozornie niewinnej kategorii urządzeń jak elektroniczne zabawki[16] czy elektroniczne nianie[17].

---

[11] M. Colesky, J.-H. Hoepman, C. Hillen, „A critical analysis of privacy design strategies", IEEE Security and Privacy Workshops, pp. 33–40, 2016; patrz też: O. Drozd, „Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC29100 into the Software Development Process", Privacy and Identity, IAICT vol. 476, pp. 129–140. Springer, 2016.

[12] J. Brookman, „Eroding Trust: How New Smart TV Lacks Privacy by Design and Transparency", IAPP, 2013, https://privacyassociation.org/news/a/erodingtrust-hownew-smart-tv-lacks-privacy-by-design-and-transparency/, patrz też: Shane Harris, „Your SmartTV is Spying on You, Basically", The Daily Beast, 2015, http://www.thedailybeast.com/articles/2015/02/05/your-samsung-smarttv-is-spyingon-youbasically.html również: https://zaufanatrzeciastrona.pl/post/szpieg-w-twoim-pokoju-o-telewizorach-sprytniejszych-od-widzow/.

[13] Przykładowo: Alexandr Railean, Delphine Reinhardt, „Life-Long Privacy in the IoT? Measuring Privacy Attitudes Throughout the Life-Cycle of IoT Devices", IFIP AICT 526, pp. 132–149, 2018; również: M. Elkhodr, et al.: „A review of mobile location privacy in the Internet of Things", 10th Int'l Conference on ICT and Knowledge Engineering, 2012.

[14] Lily Hay Newman, „Pretty Much Every Smart Home Device You Can Think of Has Been Hacked", 2014, http://www.slate.com/blogs/future_tense/2014/12/30/the_internet_of_things_is_a_long_way_from_ being_secure.html.

[15] Raport BITAG (Broadband Internet Technical Advisory Group), 2016, https://www.bitag.org/report-internet-of-thing-security-privacy-recommendations.php.

[16] Przykładowo: https://sekurak.pl/barbie-z-interfejsem-wifi-shackowana-i-przerobiona-na-szpiega/; również: https://sekurak.pl/inteligentne-misie-przejete-wyciek-800-000-kont-dostep-live-do-nagran-i-zdjec-uzytkownikow/.

[17] Loulla-Mae Eleftheriou-Smith, „Baby Monitors, CCTV Cameras and Webcams from U. Homes and Businesses Hacked and Uploaded onto Russian Website", The Independent

Szczególnie poważne zagrożenia dotyczą wszczepianych urządzeń biomedycznych (ang. *Implantable Medical Devices*,IMD), takich jak stymulatory serca, neurostymulatory, pompy insulinowe, kardiowerter-y/defibrylatory, monitory pulsu, ciśnienia, ECG, EMG itp. Większość tego typu urządzeń stosuje bardzo słabe zabezpieczenia – wystarczy wspomnieć choćby protokoły komunikacyjne bez użycia szyfrowania czy uwierzytelnianie dostępu poprzez hasła słabej jakości[18]. Całkiem realne scenariusze ataku mogą obejmować np. przypadki śmiertelnego porażenia prądem o wysokim napięciu (ok. 830V) z defibrylatora, zmianę częstotliwości pracy stymulatora serca czy wymuszenie ciągłej transmisji radiowej z urządzenia (kto wie, może nawet poprzez masowe wysyłanie spamu, w niedalekiej przyszłości?) i tym samym znacznie przyspieszone wyładowanie baterii.

Osobną kategorię zagrożeń niesie ze sobą coraz powszechniejsze monitorowanie i śledzenie obywateli. Technologia pozwala tu na bardzo wiele[19]. Reprezentatywnym przykładem mogą być podłączone do globalnej sieci samochody profilujące kierowców, przesyłające do centrów danych producenta informacje o historii wozu, w tym prędkości podróżowania, spalaniu oraz współrzędne geograficzne (tras i miejsc parkowania)[20].

Najpowszechniej dostępnymi danymi wykorzystywanymi współcześnie do śledzenia aktywności są metadane lokalizacyjne, rejestrowane m.in. wraz ze zdjęciami robionymi aparatami fotograficznymi lub telefonami wyposażonymi w układy lokalizacyjne (np. GPS lub GLONASS). Owe metadane, domyślnie zapisywane w nagłówkach plików graficznych przechowujących takie fotografie, pośród wielu różnych informacji zawierają dokładną datę zrobienia zdjęcia, współrzędne geograficzne i markę aparatu fotograficznego. Co prawda metadane lokalizacyjne można z takich plików łatwo usunąć, jednak większość z nas tego nie czyni, prawdopodobnie nie dostrzegając takiej potrzeby lub nie będąc nawet świadomymi, że taka możliwość istnieje.

(Nov. 20, 2014), http://www.independent.co.uk/life-style/gadgets-and-tech/baby-monitorscctv-cameras-and-webcams-from-uk-homes-and-businesses-hacked-and-uploaded-onto russian-website-9871830.html.

[18] https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01.

[19] J. Brookman, G.S. Hans, „Why Collection Matters: Surveillance as a De Facto Privacy Harm", 2013, http://www.futureofprivacy.org/wp-content/uploads/BrookmanWhy-Collection-Matters.pdf.

[20] M. Corkery, J. Silver-Greenberg, „Miss a Payment? Good Luck Moving That Car", The New York Times, Sept. 24, 2014, http://dealbook.nytimes.com/2014/09/24/miss-apayment-good-luck-moving-that-car/.

Z tego powodu w 2018 roku doszło do kilku incydentów związanych z nieświadomym ujawnianiem tajnych lokalizacji przez pracowników używających telefonów z GPS, w których to przypadkach tajne ośrodki wojskowe zostały niechcący zdekonspirowane przez pozornie niewinną analizę metadanych rejestrowanych przez aplikacje zainstalowane w telefonach personelu[21].

Oczywiście z metadanych od lat korzystają służby specjalne. Już Edward Snowden ujawnił, że amerykańska Agencja Bezpieczeństwa Narodowego (NSA) kataloguje fotografie wgrywane przez użytkowników Internetu do sieci i umożliwia ich przeszukiwanie pod kątem metadanych (np. „znajdź zdjęcia wykonane tym samym aparatem", „wykonane w tym miejscu")[22]. Do wiadomości publicznej przeciekły też informacje na temat programu RIOT, który profiluje obywateli na podstawie informacji zbieranych z ich profili w sieciach społecznościowych[23]. Choć zwykli obywatele nie mają dostępu do narzędzi NSA, to mogą skorzystać z co najmniej kilku dostępnych powszechnie usług pozwalających na śledzenie lokalizacji osób z wykorzystaniem np. metadanych publikowanych przez nich zdjęć. Jednym z takich serwisów jest PleaseRobMe.com, monitorujący portale społecznościowe w celu ustalenia prawdopodobnej aktualnej lokalizacji użytkowników i wychwytujący tych z nich, którzy w danej chwili znajdują się poza domem, sugerując przy okazji, czyje mieszkanie jest zatem najprawdopodobniej obecnie puste.

W sukurs zwykłym użytkownikom mogą przyjść dostępne w Internecie różne narzędzia ograniczające w dużym stopniu wycieki osobistych informacji. I tak przykładowo, ochrona przed śledzeniem jest wbudowana w niektóre przeglądarki internetowe (np. Mozilla Firefox) bądź możliwa do łatwego dodania przez zainstalowanie odpowiednich tzw. rozszerzeń przeglądarki (np. Lightbeam).

Godne szerszego polecenia jest też mobilne narzędzie SpyAware[24], przydatne do monitorowania wycieków danych dokonywanych przez aplikacje zainstalowane w telefonie. W istocie jest to aplikacja śledząca aplikacje śledzące. Jak widać, śledzenie może być bronią obusieczną,

---

[21] Przykładowo: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases. również: https://www.bellingcat.com/resources/articles/2018/07/08/ strava-polar-revealing-homes-soldiers-spies/.

[22] https://niebezpiecznik.pl/post/xkeyscore-jeszcze-gorszy-niz-prism-czyli-nsa-zbiera-wszystko-co-robisz-w-sieci/.

[23] https://niebezpiecznik.pl/post/riot-rzadowy-system-inwigilacji-przez-serwisy-spolecznosciowe/.

[24] https://play.google.com/store/apps/details?id=com.ls.android.threatmonitor.

toteż warto choć od czasu do czasu spróbować użyć jej na własną korzyść.

Szczęśliwie dla nas wszystkich można już zaobserwować pewne próby podejmowania wysiłków zmierzających do ustanowienia branżowych standardów[25] odnośnie do takiej budowy produktu i wytwarzania oprogramowania, aby wykluczyć lub zminimalizować zagrożenia, na jakie narażone są współcześnie (i potencjalnie również w najbliższej przyszłości) dane przetwarzane przez te produkty. Mowa przykładowo o metodologii DPbD (ang. *Data Protection by Design and by Default*)[26] odpowiadającej oczekiwaniom zdefiniowanym m.in. w art. 35 dyrektywy RODO i określanym wspólną nazwą *Privacy Enhancing Technologies*. Aby jednakże doczekać się praktycznych wyników w tej materii, wymagana będzie niewątpliwie nie tylko dobra wola inżynierów i programistów, ale jeszcze wola polityczna i silna presja społeczna.

[25] S. Brooks et al., „An Introduction to Privacy Engineering and Risk Management in Federal Systems", National Institute of Standards and Technology Internal Report 8062, 2017 patrz też: G. Danezis et al., „Privacy and data protection by design – from policy to engineering", European Union Agency for Network and Information Security, 2014

[26] K. Rommetveit, A. Tanas, N. van Dijk, „Data Protection by Design: Promises and Perils in Crossing the Rubicon Between Law and Engineering", IFIP AICT 526, pp. 25–37, 2018

CZŁOWIEK W CYBERŚWIECIE: CIEMNE I JASNE STRONY TECHNOLOGII

Maciej Miłostan

Politechnika Poznańska

Postęp technologiczny powoduje zwykle poprawę warunków życia człowieka, zwiększa komfort funkcjonowania zarówno indywidualnych jednostek, jak i całych społeczeństw. Jednak patrząc z perspektywy historycznej, łatwo zauważyć, że dzieła nauki i techniki niejednokrotnie znajdują zastosowanie do mniej szczytnych celów, a niekiedy wręcz są tworzone z myślą o tym, by szkodzić człowiekowi. Dobrym punktem odniesienia są w tym przypadku technologie militarne, które z założenia tworzy się tak, aby były możliwie destrukcyjne dla potencjalnego wroga.

Przy czym postęp uzyskany w technologiach wojskowych niejednokrotne przekłada się na postęp w technologiach cywilnych, dobrym przykładem jest tu energetyka jądrowa – najpierw do użycia weszła bomba atomowa[1], a następnie skonstruowano stosunkowo bezpieczne reaktory wykorzystywane do wytwarzania energii elektrycznej[2].

Niektóre technologie mogą mieć jednocześnie zastosowanie w sektorze cywilnym oraz militarnym, co świetnie obrazuje wynalazek Nobla – dynamit[3].

---

[1] „Trinity Test – 1945", Atomic Heritage Foundation, http://www.atomicheritage.org/history/trinity-test-1945 (dostęp 15.11.2019).

[2] „First nuclear power", Oak Ridge National Laboratory, https://www.ornl.gov/blog/ornl-reporter/first-nuclear-power (dostęp 15.11.2019).

[3] Marc Lallanilla, „The Dark Side of the Noble Prizes", https://www.livescience.com/40188-dark-history-alfred-nobel-prizes.html (dostęp 14.01.2020).

Dobrym przykładem różnorodnego sposobu wykorzystania tej samej technologii jest również broń palna[4], której używa się zarówno do polowań, obrony własnej, jak i do siania terroru przez zorganizowane grupy przestępcze lub organizacje paramilitarne.

Przytaczając te przykłady, zmierzamy do tego, że technologia – niezależnie od tego, w jakim celu pierwotnie została stworzona – sama w sobie zwykle nie jest ani zła, ani dobra, dopiero sposób jej wykorzystania sprawia, że odbieramy ją pozytywnie lub negatywnie. Technologia pierwotnie stworzona dla dobrych celów może zostać wykorzystana w złych intencjach i *vice versa*.

Przyjrzyjmy się teraz temu, jakie technologie stanowią podstawy współczesnego cyberświata, świata, w którym komunikujące się urządzenia cyfrowe grają pierwsze skrzypce i stanowią podstawę do tworzenia nowych usług. Nie można zaprzeczyć, że weszliśmy w erę powszechnej cyfryzacji[5] rozmaitych aspektów życia i aktualnie świat cyfrowy, wirtualny, coraz bardziej splata się ze światem fizycznym. Technologie, z których na co dzień korzystamy, są dla nas z jednej strony wybawieniem, a z drugiej zagrożeniem. Mogą one być stosowane z korzyścią dla nas, w uczciwym celu, jak również w celach przestępczych lub w celu ograniczania swobód obywatelskich. Właściwie stosowane stanowią element systemu bezpieczeństwa chroniącego indywidualne osoby lub systemy, a nadużywane są środkiem umożliwiającym osiąganie wymiernych korzyści przez grupy przestępcze, lobbystów lub rządzących (zwłaszcza w państwach niedemokratycznych). Przeanalizujmy kilka przykładów technologii i związanych z nimi zagrożeń.

Za pierwszy przykład niech posłużą nam tzw. zapory sieciowe (ang. *firewall*[6]). Blokują one, selektywnie, połączenia wychodzące i przychodzące, w pewnych podsieciach lub na pojedynczych komputerach, i są powszechnie wykorzystywane do ochrony infrastruktury sieciowej przed atakami oraz przejmowaniem zasobów komputerowych przez hakerów, w tym przed wykorzystywaniem łącz do rozsyłania niechcianej korespondencji. Dla przykładu, blokada protokołu SMTP i komunikacji na porcie 25 u większości dostawców Internetu ogranicza propagację tzw. spamu. Zapory wymyślono po to, by chronić sieci korporacyjne

[4] „Firearms", History.com, https://www.history.com/topics/inventions/firearms (dostęp 14.01.2020).

[5] „Od papierowej do cyfrowej Polski", Ministerstwo Cyfryzacji RP, https://www.gov.pl/web/cyfryzacja/od-papierowej-do-cyfrowej-polski (dostęp 14.01.2020).

[6] „Firewall", Wikipedia, https://en.wikipedia.org/wiki/Firewall_(computing) (dostęp 14.01.2020).

i indywidualnych użytkowników Internetu poprzez ograniczenie ich ekspozycji na zagrożenia. Jednakże Iran i Chiny wykorzystują tę samą technologię do skutecznego ograniczania kontaktów własnych obywateli z resztą świata[7], głównie ze światem zachodnim. Tak zwany Wielki Chiński Firewall[8] utrudnia dostęp do stron uznanych przez cenzurę za zakazane, np. popularnych usług firmy Google. Podobnie sprawy mają się w Iranie, tam również obywatele nie mają swobodnego dostępu do światowego Internetu. Rosja natomiast głośno mówi o tworzeniu własnego „Internetu" z możliwością odseparowania od sieci międzynarodowej[9], tu oficjalnym celem jest lepsza „ochrona" własnych obywateli, a w praktyce lepsza kontrola nad obywatelami i treściami, do których mają oni dostęp.

W odpowiedzi na próby inwigilacji i ograniczania dostępu do zasobów zaproponowano wiele rozwiązań mających na celu ochronę prywatności i danych, a także umożliwiających obejście zapór sieciowych. Do portfolio powszechnie stosowanych rozwiązań możemy zaliczyć szyfrowanie kanałów komunikacyjnych (i dysków)[10], enkapsulację czy tunelowanie ze szczególnym uwzględnieniem wirtualnych sieci prywatnych (VPN)[11], jak również sieci węzłów pośredniczących ze specjalnie skonstruowanymi mechanizmami routingu (wyboru tras pakietów), opartymi na algorytmach kryptograficznych – przykładem takiego rozwiązania jest Tor[12].

Innymi słowy, wraz ze wzrostem świadomości zagrożeń zarówno wśród użytkowników Internetu, jak i decydentów, zaczęto projektować i wdrażać systemy lepiej chroniące dane na różnych etapach przetwarzania. Podstawowym mechanizmem zabezpieczania danych przesyłanych kanałami komunikacyjnymi i przechowywanych w systemach komputerowych są algorytmy kryptograficzne umożliwiające szyfrowanie danych. W chwili obecnej stosuje się dwie główne klasy tych algorytmów: symetryczne i asymetryczne. Te drugie, zwane również

---

[7] „Cenzura w Internecie", Wikipedia, https://pl.wikipedia.org/wiki/Cenzura_w_Internecie (dostęp 14.01.2020).

[8] „The Great Firewall of China", Bloomberg News, https://www.bloomberg.com/quicktake/great-firewall-of-china (dostęp 14.01.2020).

[9] M. Domańska, „Twierdza Runet: walka Kremla z „wrogim" Internetem", Ośrodek Studiów Wschodnich, https://www.osw.waw.pl/pl/publikacje/analizy/2019-04-19/twierdza-runet-walka-kremla-z-wrogim-internetem (dostęp 14.01.2020).

[10] „OpenSSL", OpenSSL Software Foundation, https://www.openssl.org/ (dostęp 14.01.2020).

[11] „VPN Gate Overview", University of Tsukuba, Japan, https://www.vpngate.net/en/about_overview.aspx (dostęp 14.01.2020).

[12] Tor Project, https://www.torproject.org/ (dostęp 14.01.2020).

algorytmami z kluczem jawnym, tworzą podstawy tzw. infrastruktury klucza publicznego[13] (PKI – *Public Key Infrastucture*). W przypadku tej grupy algorytmów mamy do czynienia z parą kluczy – jeden klucz (zwany publicznym) jest powszechnie znany i wykorzystywany do szyfrowania wiadomości, a drugi jest tajny i służy do deszyfrowania wiadomości. Konstrukcja algorytmu zwykle dopuszcza możliwość zamiany kluczy i wykorzystanie klucza prywatnego do szyfrowania, a publicznego do deszyfrowania, co stanowi podstawę podpisów elektronicznych. Gwarantem bezpieczeństwa takiego systemu kryptograficznego jest złożoność obliczeniowa operacji, w której można z klucza publicznego wygenerować klucz prywatny. Innymi słowy, wyliczenie klucza prywatnego z publicznego zajmuje bardzo dużo czasu, w praktyce powinno trwać dłużej niż wynosi „okres przydatności" zaszyfrowanej wiadomości.

PKI jest powszechnie wykorzystywana w podpisach cyfrowych i to ona umożliwia m.in. dostarczanie certyfikatów SSL używanych do zabezpieczania stron WWW. Dzięki certyfikatom przeglądarka jest w stanie potwierdzić tożsamość witryny na podstawie łańcucha zaufania i poinformować użytkownika, że łączy się ze zweryfikowaną witryną – świadczy o tym symbol kłódki wyświetlany przy pasku adresu. Weryfikacja tożsamości jest możliwa, gdyż przeglądarka jest dystrybuowana z certyfikatami zaufanych centrów certyfikacji (CA), które to centra wystawiają certyfikaty SSL dla konkretnej witryny. Certyfikaty CA zainstalowane w przeglądarce dają możliwość stwierdzenia, czy certyfikat, którym przedstawia się witryna, został podpisany przez zaufaną stronę trzecią.

Łatwo zauważyć, że kluczowe jest tutaj zaufanie do dostawców oprogramowania (przeglądarek) oraz centrów certyfikacji. Niestety rzeczywiste przypadki pokazują, że nie zawsze możemy w pełni ufać stronom trzecim. W roku 2018 firma DigiCert (będąca CA) anulowała ponad 20 tys. certyfikatów SSL[14], po tym jak wyciekły klucze prywatne z nimi powiązane. Podobny przypadek odnotowano w roku 2011[15], lecz wówczas wyciekł klucz wykorzystywany do podpisywania certyfikatów

[13] „Infastruktura Klucza Publicznego", Wikipedia, https://pl.wikipedia.org/wiki/Infrastruktura_klucza_publicznego (dostęp 14.01.2020).

[14] Adam Haertle „Jaka piękna katastrofa...", Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/post/jaka-piekna-katastrofa-czyli-czego-nie-robic-z-certyfikatami-ssl/ (dostęp 14.01.2020).

[15] Dennis Fisher „Final Report on DigiNotar Hack Shows Total Compromise of CA Servers", Threatpost.com https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/ (dostęp 14.01.2020).

przez DigiNotar, co umożliwiło wygenerowanie sfałszowanych certyfikatów. W oparciu o te certyfikaty przeprowadzono szereg ataków typu *man-in-the-middle*[16] na użytkowników serwisów internetowych. W tym przypadku ślad prowadził w stronę wywiadu irańskiego, a także NSA. Nikogo nie skazano, a dostawcy przeglądarek wprowadzili certyfikaty DigiNotar na czarną listę. DigiNotar ogłosiło bankructwo w niedługim czasie po ujawnieniu incydentów.

Podsumowując, mechanizmy szyfrowania asymetrycznego są wykorzystywane do weryfikacji tożsamości, natomiast szyfrowanie symetryczne, w powiązaniu z algorytmami uzgadniania czy wymiany klucza (takim jak np. algorytm Diffiego-Hellmana), są wykorzystywane do szyfrowania kanałów komunikacyjnych – algorytmy asymetryczne są do tego celu za wolne (wymagają znacznych nakładów obliczeniowych). W przypadku algorytmów uzgadniania klucza dwie strony mogą ustalić wspólny klucz poprzez niezabezpieczony kanał komunikacyjny bez ryzyka ujawnienia go stronom trzecim, mającym możliwość podsłuchiwania wszystkich komunikatów. Wykorzystuje się do tego odpowiednią sekwencję ustalonych operacji matematycznych.

Jednakże i w przypadku stosowania algorytmów wymiany klucza nie możemy czuć się w pełni bezpieczni lub pewni, że nikt nas nie podsłuchuje – otóż w 2015 roku pokazano, że fakt, iż wiele implementacji algorytmu Diffiego-Hellmana używa tych samych liczb pierwszych, daje, w znacznej liczbie przypadków, agencjom dysponującym dużą mocą obliczeniową możliwość przeprowadzania ataku polegającego na wyliczeniu wartości klucza. Dodatkowo słabość w implementacji tego protokołu, wymuszona restrykcjami eksportowymi wprowadzonymi w latach 90. XX wieku przez USA, umożliwiała obniżenie długości liczb pierwszych używanych w tym protokole do 512 bitów. W ataku typu MITM (*man-in-the-middle*), czyli z udziałem „osoby" pośredniczącej, która może zmodyfikować początkowe komunikaty w trakcie negocjacji połączenia, podatność tę nazwano LOGJAM[17].

Stosowanie technik kryptograficznych ma za zadanie zapewnić poufność przesyłanych danych, natomiast to, jakie dane są przesyłane, zależy tylko i wyłącznie od użytkowników technologii. Mogą to być treści związane z finansami (np. dostęp do systemów bankowych), dane medyczne, dane stanowiące tajemnicę danej firmy, ale mogą to być również treści związane z działalnością przestępczą, terroryzmem.

[16] Atak typu *man-in-the-middle*, to atak, w którym osoba trzecia może przechwytywać i modyfikować dane przesyłane pomiędzy dwoma komunikującymi się stronami.
[17] „Weak Diffie-Hellman and the Logjam Attack", https://weakdh.org/ (dostęp 14.01.2020).

Innymi słowy, technologia ta służy zarówno zwykłym obywatelom, jak i przestępcom. Treści zaszyfrowanych zwykle nie można w prosty sposób filtrować czy przeglądać ich zawartości bez uprzedniego odszyfrowania, co komplikuje ochronę sieci korporacyjnych i infrastruktury sieciowej, a także może utrudniać działania policji i innym służbom śledczym. Notabene niektóre rządy (np. USA) nakładają w związku z tym embarga na transfery technologii wykorzystujących silne mechanizmy kryptograficzne – tak, aby służby mogły złamać szyfry w akceptowalnym czasie. W niektórych przypadkach w środowiskach korporacyjnych dokonuje się odszyfrowywania ruchu na firewallu i przeprowadza się klasyczną inspekcję zawartości pakietów, ale wymaga to odpowiedniej konfiguracji komputerów klienckich i całej infrastruktury sieciowej.

Stosowanie szyfrowanych kanałów komunikacyjnych ogranicza możliwość infiltracji różnych środowisk, ale nie wyeliminowuje tej możliwości w 100% – nadal można ustalić np. między jakimi adresami IP zestawione zostało połączenie lub kto do kogo i kiedy dzwonił, a co za tym idzie, zawęzić grono podejrzanych, jeśli transmisja lub rozmowa miała związek z działalnością przestępczą lub działalnością stanowiącą zagrożenie w oczach rządzących. W oparciu o logi połączeń czy dane billingowe nadal można próbować szukać powiązań pomiędzy komunikującymi się osobami. Oliwy do ognia dodaje fakt, że również biblioteki kryptograficzne mogą zawierać błędy umożliwiające ataki na komputery z nich korzystające i ich użytkowników. Wykryta w 2014 roku w bibliotece OpenSSL (jednej z najpowszechniej stosowanych bibliotek kryptograficznych na świecie) luka HeartBleed[18] umożliwiała zdalne pozyskanie fragmentów pamięci serwerów używających podatnej na ataki biblioteki. W pamięci można było znaleźć klucze prywatne i ciasteczka sesyjne użytkowników, co umożliwiało dalsze ataki. Błąd wykryto dopiero po dwóch latach od jego wprowadzenia do kodu źródłowego biblioteki. Kolejny błąd (POODLE[19]) w konstrukcji protokołu SSLv3 doprowadził do gwałtownego zaprzestania korzystania z niego. Atak w skrócie umożliwiał przejęcie sesji użytkowników.

Wracając do inwigilacji użytkowników, to nawet przy założeniu, że korzystamy z bezpiecznych bibliotek, możliwe jest analizowanie danych o połączeniach – adresy źródłowe i docelowe w protokole TCP/IP nie są szyfrowane. Dlatego, w celu zwiększenia stopnia prywatności (anonimizacji

[18] The Heartbleed Bug, http://heartbleed.com/ (dostęp 14.01.2020).

[19] „SSLv3 umarł. Zjadł go pudel.", Niebezpiecznik.pl, https://niebezpiecznik.pl/post/sslv3-umarl-zjadl-go-pudel/ (dostęp 14.01.2020).

informacji o połączeniach) i ograniczenia możliwości inwigilacji, wprowadzono szereg kolejnych, dodatkowych mechanizmów, do których zalicza się technologię wirtualnych sieci prywatnych (VPN). Została ona zaprojektowana głównie po to, by dać możliwość podłączania się do sieci korporacyjnych przez pracowników pracujących w terenie lub z domu, lecz szybko została zaadaptowana do celów związanych z ukrywaniem własnej tożsamości. W VPN cały ruch do określonych sieci jest przesyłany (tunelowany) przez pojedynczy host pośredniczący, do którego to hosta ruch odbywa się kanałem szyfrowanym. VPN jest dość często wykorzystywany do obchodzenia cenzury lub ukrywania źródeł ataku. W tych przypadkach zwykle wykorzystuje się serwery VPN umieszczone w sieciach, których operatorzy nie są skorzy do współpracy z organami ścigania i/lub znajdują się w innym kraju niż osoba prowadząca zabronioną działalność. Organy ścigania mają mocno ograniczone pole działania, jeśli atak pochodzi z kraju, z którym nie mają ustalonych procedur współpracy lub brak jest możliwości prawnych na podjęcie interwencji. W niektórych przypadkach wykorzystanie pojedynczego hosta pośredniczącego to za mało do skutecznego ukrycia prawdziwej tożsamości – znaczenie tu ma, gdzie znajdują się cele i źródła ataku i kto ma dostęp do danych o połączeniach. Poprzez korelację wolumenów ruchu, czasu i informacji o adresach źródłowych i docelowych operator może dokonać deanonimizacji połączeń.

W latach 90. XX wieku rozpoczęto pracę nad rozwiązaniami, które umożliwiłyby skuteczne ukrywanie tożsamości komunikujących się stron nawet przed operatorami mającymi możliwość monitorowania aktywności poszczególnych użytkowników sieci. W efekcie powstał Tor – system, który wykorzystuje szereg węzłów pośredniczących i mechanizmy szyfrowania asymetrycznego w protokole routingu, tak aby każdy węzeł znał tylko bezpośredniego poprzednika i następcę w łańcuchu połączeń. Informacje o wszystkich hostach pośredniczących są szyfrowane z użyciem algorytmów asymetrycznych, aby możliwe było przesłanie komunikatów zwrotnych. System jest wyposażony w dedykowaną przeglądarkę internetową (Tor Browser), która daje możliwość wyboru punktów wejścia i wyjścia z sieci Tor (np. wskazanie kraju), pozwalając na zachowanie anonimowości przy dostępie do zasobów internetowych lub omijanie ograniczeń terytorialnych. Ograniczenia terytorialne są często stosowane np. przez dostawców multimediów (wideo na żądanie (VOD), telewizja on-line). Dedykowana przeglądarka ma ograniczoną liczbę wtyczek, aby zminimalizować ryzyko ujawnienia oryginalnego adresu IP klienta, w szczególności

standardowo blokowany jest Flash i odtwarzacze multimediów, takie jak RealPlayer oraz Quicktime.

Teoretycznie Tor zapewnia dość dużą anonimowość, ale w niektórych scenariuszach istnieje możliwość zidentyfikowania osoby, która z niego korzysta. Dla przykładu na Harvardzie jeden ze studentów, łącząc się przez Tora, wszczął fałszywy alarm bombowy, wysyłając e-maila z jednorazowej skrzynki[20]. Pech chciał, że student, który to zrobił, był jedynym użytkownikiem, który łączył się z Torem z uniwersyteckiej sieci wi-fi w momencie wysłania zgłoszenia i stosunkowo łatwo udało się go namierzyć na podstawie logów uniwersyteckich systemów komputerowych. Student przyznał się do zarzucanych mu czynów[21].

Sieć Tor umożliwia również udostępnianie w sposób anonimowy stron internetowych[22]. Do tego celu przewidziano specjalny protokół (Onion Service Protocol), który umożliwia rejestrację usług w sieci Tor bez ujawniania własnej tożsamości. Udostępniana usługa otrzymuje identyfikator w specjalnej domenie .onion. W sieci Tor nie ma klasycznych wyszukiwarek internetowych, takich jak np. Google. Wymiana informacji o udostępnianych stronach odbywa się w taki sam sposób jak w początkowym okresie funkcjonowania Internetu, aczkolwiek pojawiają się katalogi stron tworzone mniej lub bardziej automatycznie. Anonimowość zapewniana przez sieć Tor powoduje, że ukryte zasoby, strony i usługi w niej udostępniane są często wykorzystywane przez przestępców i z tego względu noszą miano „ciemnej sieci" – Dark Web. W Dark Web można znaleźć zarówno treści, które są w pełni legalne, np. kluby książki czy portale informacyjne umożliwiające swobodną wymianę opinii w poczuciu pełnej wolności słowa, jak również cały szereg portali służących działalności przestępczej. Dla przykładu na portalach w Dark Web można uzyskać dostęp do skradzionych danych, takich jak hasła do przejętych kont na portalach, numery identyfikacyjne (np. Social Security Number), numery kart kredytowych. Istnieją tam również platformy, na których można nabyć nielegalne substancje, np. narkotyki, leki bez posiadania stosownej recepty oraz środki toksyczne. Ponadto dystrybuowane są tam również

[20] R. Brandom, „FBI agents tracked Harvard bomb threats despite Tor", https://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor (dostęp 14.01.2020).

[21] P. Vogt, „That Bomb-Hoaxing Harvard Student Was Using Tor, But They Caught Him Anyway", https://www.wnyc.org/story/harvard-bomb-threat/ (dostęp 14.01.2020).

[22] K. Rankin„Tor Hidden Services", https://www.linuxjournal.com/content/tor-hidden-services (dostęp 14.01.2020).

treści zabronione, takie jak pornografia dziecięca czy mniej kontrowersyjne materiały chronione prawami autorskimi. Można zamówić ataki cybernetyczne, np. tzw. DDoS – ataki wykorzystujące sieci botnetów (zainfekowanych komputerów) w celu zalania dużym wolumenem ruchu serwisów będących celem ataku i przez to uniemożliwienie ich normalnego funkcjonowania. Z bardziej drastycznych zastosowań należy wymienić handel ludźmi czy handel organami do przeszczepów bądź świadczenie usług kryminalnych (płatne morderstwa, pobicia).

Rozkwit przestępczej działalności ułatwiają kryptowaluty[23] – wirtualne waluty bazujące na mechanizmach kryptograficznych i rejestrach rozproszonych, które miały dać społeczeństwom możliwość swobodnej wymiany kapitału i realizowanie płatności w sposób niezależny od jakichkolwiek rządów, instytucji regulujących przepływy finansowe czy operatorów kart płatniczych. Miały dać jednostkom swobodę handlu na arenie międzynarodowej bez konieczności uiszczania drakońskich opłat transakcyjnych, opłat za przelewy międzynarodowe czy uwzględniania różnic kursowych pomiędzy cenami kupna i sprzedaży (tzw. *spread*). Pierwszą i jednocześnie najszerzej rozpoznawalną kryptowalutą jest Bitcoin[24]. Intencje wprowadzenia tego rodzaju środkach płatniczego były dobre, ale kryptowaluty szybko zostały docenione przez przestępców i umożliwiły rozkwit nielegalnego handlu, stając się znakomitym uzupełnieniem sieci Dark Web. Zostały one również docenione przez twórców wirusów szyfrujących dyski i żądających okupu[25] (tzw. *ransomware*) – okup za odszyfrowanie dysku płaci się kryptowalutami. Początkowo entuzjastyczny stosunek do kryptowalut z czasem nieco osłabł – kryptowaluty zamiast szeroko trafić pod strzechy, stały się narzędziem w rękach spekulantów. Wprawdzie nadal się dużo o nich mówi i próbuje je wdrażać w sposób bardziej kontrolowany, ale ich adopcję znacznie utrudnia niejasny status legislacyjny. Co ciekawe, nad własną, globalnie stabilną kryptowalutą pracuje Facebook, ale w ostatnich miesiącach stracił wsparcie ze strony wiodących instytucji finansowych z grupy G20 oraz Visy i MasterCard[26].

---

[23] „Kryptowaluta", Wikipedia, https://pl.wikipedia.org/wiki/Kryptowaluta (dostęp 14.01.2020).

[24] Bitcoin, Bitcoin.org, https://bitcoin.org/pl/jak-to-dziala (dostęp 14.01.2020).

[25] Michael Baker, „How Cryptocurrencies Are Fueling Ransomware Attacks And Other Cybercrimes", Forbes, https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/ (dostęp 14.01.2020).

[26] Leo Jakobson, „With stablecoin ban, G20 deals Facebook's Libra ambitions another blow", https://modernconsensus.com/regulation/with-stablecoin-ban-g20-deals-facebooks-libra-ambitions-another-blow/ (dostęp 14.01.2020).

Mniej kontrowersji wzbudza technologia wywodząca się z kryptowalut, a mianowicie technologia *blockchain* (łańcuch bloków). Technologia *blockchain* umożliwia tworzenie rozproszonych, redundantnych rejestrów i odnotowywanie wszelkich zmian wprowadzanych do składowanych w nich danych. Rejestry tworzone z użyciem technologii *blockchain* powinny być niemutowalne – raz dodany blok powinien pozostawać niezmieniony, dlatego próbuje się je stosować do implementacji rejestrów, które z założenia przechowują dane permanentnie (np. księgi katastralne). Problem jednak w tym, że w przypadku przejęcia lub wprowadzenia do systemu wystarczająco dużej liczby węzłów (w przypadku Bitcoina jest >50% mocy obliczeniowej) można zmodyfikować bloki, które już się w łańcuchu bloków znajdują. Kolejnym problemem jest permanentne przechowywanie wszystkich bloków, co może w niektórych zastosowaniach rodzić problemy z ochroną danych osobowych i praw jednostek. Dość poważnym zarzutem kierowanym w kierunku tej technologii jest także jej ślad energetyczny i rozmiar wolumenów dyskowych (te same dane są zduplikowane na wielu węzłach). Warto jednak zaznaczyć, że mimo swoich ograniczeń *blockchain* pozostaje obiecującą technologią o dużym potencjale.

Przejdźmy teraz do innego rodzaju zagrożenia, a mianowicie wycieków danych czy przejmowania systemów na skutek błędów w aplikacjach, usługach czy systemach operacyjnych. Popełnianie błędów jest rzeczą ludzką i programiści, projektanci oraz administratorzy systemów informatycznych nie są tutaj wyjątkiem. W efekcie dochodzi do znajdywania w systemach luk, które czynią je podatnymi na ataki, umożliwiając dla przykładu przejęcie kont użytkowników lub kradzież danych składowanych w systemie (w tym np. skrótów haseł bądź wręcz całych haseł). M.in. z tego względu zaleca się stosowanie różnych haseł do różnych portali. Błędy występują również w oprogramowaniu klienckim, np. w przeglądarkach internetowych czy ich wtyczkach (np. Flash czy Java), i umożliwiają infekcję komputera w przypadku wejścia na specjalnie spreparowaną stronę. Podatności w oprogramowaniu biurowym mogą również zostać wykorzystane do przejęcia komputera – wystarczy, że użytkownik otworzy specjalnie spreparowany załącznik do e-maila. Współczesne edytory tekstów, jak np. Microsoft Word, umożliwiają stosowanie automatyzacji w postaci makr lub osadzanie bardziej złożonych obiektów, co rozszerza spektrum potencjalnych scenariuszy ataków. Podatności w przeglądarkach internetowych umożliwiały wykorzystanie do infekcji komputerów nawet plików graficznych, takich jak np. jpg. Co ciekawe, podatności w systemach zarządzania treścią na serwerach i oprogramowaniu klienckim niekiedy

bywają wykorzystywane przez cyberpolicję – dobrym przykładem jest tu akcja wymierzona przeciwko pedofilom, przeprowadzona przez policję holenderską. Policjanci przejęli forum w Dark Web i zainfekowali je własnym trojanem, który automatycznie instalował się na komputerach przestępców je odwiedzających. Operacje nosiła kryptonim „torpedo"[27]. Warto wspomnieć, że dla zwykłych użytkowników Internetu zagrożenie stanowią również firmy świadczące usługi tak zwanego „kuloodpornego" hostingu („bulletproof" hosting), który daje możliwość hostowania serwerów z praktycznie dowolną nielegalną zawartością (choć tu niektóre firmy wprowadzają pewne ograniczenia przynajmniej w oficjalnych regulaminach) i podejmowania z nich działań przestępczych. Firmy świadczące tego typu usługi starają się skutecznie utrudniać pracę policji, ale i w walce z nimi służby odnoszą sukcesy, co pokazuje akcja niemieckiej policji z września 2019 roku[28].

Wśród użytkowników Internetu wzrasta świadomość zagrożeń wynikających z używania niewłaściwie zabezpieczonego sprzętu lub oprogramowania podatnego na ataki. Warto zauważyć, że możliwość wystąpienia błędu czyniącego oprogramowanie podatnym na atak jest trudna do uniknięcia, można co najwyżej ograniczać ryzyko wystąpienia takich błędów. Oprogramowanie jest tworzone przez zespoły programistyczne o różnych kwalifikacjach, często w sposób modularny i naturalną (typowo ludzką) rzeczą jest, że w implementacjach pojawiają się błędy, które wykrywane są już po powszechnym wdrożeniu produktu i integracji niezależnych modułów. Zatem to, co można robić, to dostarczać mechanizmy pozwalające na właściwe adresowanie problemów bezpieczeństwa w krótkim czasie. Do tego służą systemy automatycznych aktualizacji. Dzięki tym systemom ograniczamy możliwość ataku na nasze zasoby, ale jednocześnie dajemy dostawcom możliwość oprogramowania dystrybucji dowolnych kodów, które mogą w pewnym momencie (np. konflikt militarny) zostać wykorzystane przeciwko nam. Zdarza się również, że nowe aktualizacje jednego producenta nie są w pełni kompatybilne z użytkowanym przez nas oprogramowaniem innego lub nawet tego samego producenta. Idea zatem jest jak najbardziej właściwa, ale w niektórych zastosowaniach należy zachować ostrożność. Warto tu przywołać rok 2016 i skandal z oprogramowaniem do zdalnej aktualizacji firmware-u (z ang. FOTA – *Firmware Over The Air*) na telefonach

[27] Operacja torpedo, https://www.wired.com/2014/08/operation-torpedo/ (dostęp 14.01.2020).
[28] Brian Krebs „German Cops Raid „Cyberbunker 2.0," Arrest 7 in Child Porn, Dark Web Market Sting" https://krebsonsecurity.com/2019/09/german-cops-raid-cyberbunker-2-0-arrest-7-in-child-porn-dark-web-market-sting/ (dostęp 14.01.2020).

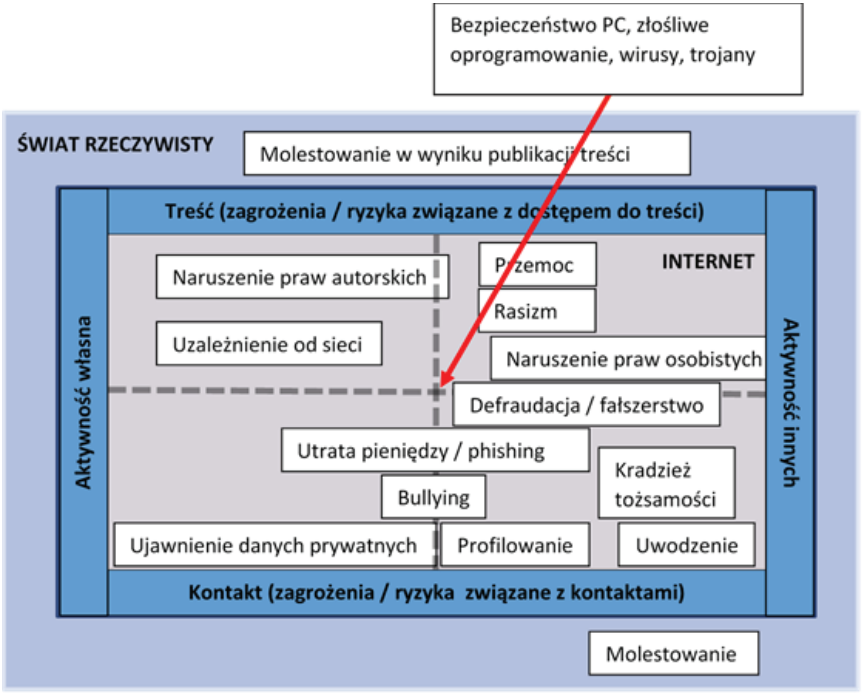
komórkowych, który pokazał, że niekiedy systemy automatycznej aktualizacji mogą ujawniać więcej danych, niż byśmy sobie tego życzyli. W tym przypadku dostawca oprogramowania do aktualizacji, tj. chińska firma ADUPS, zbierała m.in. dane o identyfikatorach stacji bazowych, do których telefon się łączył, połączeniach, a także zawartości wiadomości SMS. Oprogramowanie było wykorzystywane na ponad 150 modelach telefonów sprzedawanych na całym świecie, aczkolwiek początkowo mówiono tylko o urządzeniach firmy BLU (dystrybuowanych m.in. przez Amazona). Do czego firma wykorzystywała te dane w praktyce nie wiadomo, przy czym w oficjalnym komunikacie, opublikowanym po ujawnieniu problemu, zastrzega, że nie dzieliła się tymi danymi z firmami trzecimi ani agencjami rządowymi. W przypadku systemów automatycznej aktualizacji, podobnie jak w przypadku systemów chmurowych czy platform usługowych i społecznościowych, pojawia się kwestia zaufania – komu ufamy i jakie dane mu powierzamy.

Inwencja cyberprzestępców w tworzeniu nowych ataków i kreatywne wykorzystywanie wszystkich dostępnych, często z pozoru niegroźnych, zasobów bywa zaskakująca, co pokazują wolumenowe ataki wielkoskalowe (typu DRDoS) poważnie zakłócające pracę operatorów sieci i serwisów internetowych. Dla przykładu do przeprowadzenia dużego ataku na portal KrebsOnSecurity wykorzystano botnet (zwany Mirai), stworzony z niezabezpieczonych kamer podłączonych do sieci Internet[29]. Do ataków na sieć Sony PlayStation i Microsoft (serwisy związane z Xbox-em) wykorzystano routery domowe, które miały „dziurawe" oprogramowanie układowe (*firmware*)[30]. W amplifikacji ataków powszechnie wykorzystuje się również popularne serwery usług, np. serwery nazw, serwery czasu (NTP) czy serwery usług katalogowych (LDAP). Najłatwiej do tego wykorzystać serwery, które operują w oparciu o protokół UDP, gdyż w ich przypadku istnieje możliwość sfałszowania adresu nadawcy, który odpowiada adresowi serwera ofiary. Ofiara (serwer) zostaje zalana odpowiedziami, których się nie spodziewa i w krytycznym przypadku dochodzi do wysycenia łącza lub zasobów, co prowadzi do niedostępności usługi.

[29] B. Kerbs, „Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K", https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/ (dostęp 14.01.2020).

[30] Ch. Brook, „Lizard Squad's DDoS-For-Hire Service Built on Hacked Home Routers" https://threatpost.com/lizard-squads-ddos-for-hire-service-built-on-hacked-home-routers/110341/ (dostęp 14.01.2020).

Łatwo zauważyć, że większość niebezpieczeństw i zagrożeń nie wynika z samej technologii, a z niewłaściwego jej wykorzystywania przez osoby o złych intencjach oraz w mniejszym stopniu od czynników losowych (np. awarie, katastrofy naturalne, wypadki). Biorąc ten aspekt pod uwagę, możemy zdefiniować katalog zagrożeń przez pryzmat kilku podstawowych czynników, to jest: treści, które publikujemy, konsumujemy lub przesyłamy; kontaktów, które nawiązujemy przy pomocy Internetu; oraz aktywności naszej i cudzej. Klasyfikację zagrożeń opartych na tych trzech czynnikach nazywa się modelem 3Cs (ang. *content* (treść), *contact* (kontakt), *condact* (postępowanie)). Model ten pozwala podejść metodycznie do charakterystyki zagrożeń (por. rys. 1), na które są narażeni użytkownicy Internetu i stosuje się go zwłaszcza w kontekście korzystania z sieci przez osoby małoletnie.



Rys. 1. Model klasyfikacji zagrożeń 3Cs

(źródło: I.R. Berson, M.J. Berso, „High-tech Tots: Childhood in a Digital World", Information Age Publishing, 2010.)

Katalog zagrożeń obejmuje takie aspekty, jak: *bullying*, czyli znęcanie się czy zastraszanie najczęściej przez grupę rówieśniczą; uwodzenie i molestowanie, w tym wykorzystanie nieletnich; naruszanie praw osobistych, oszczerstwa, mowa nienawiści; rasizm; nawoływanie do przemocy; narażenie na oglądanie treści niedostosowanych do wieku; malwersacje, oszustwa, w tym *phishing* i kradzieże tożsamości, podszywanie się; utrata prywatności; kradzieże praw majątkowych, np. praw autorskich.

W tym kontekście niestety należy ze smutkiem stwierdzić, że największym zagrożeniem w cyberświecie nie jest technologia, a drugi człowiek. Cyberświat jest lustrzanym odbiciem świata rzeczywistego, przy czym w tym odbiciu zarówno aspekty pozytywne, jak i negatywne ulegają wyjaskrawieniu. Na szczęście części zagrożeń możemy unikać, podobnie jak w świecie rzeczywistym, nie szukając miejsc, w których nie chcielibyśmy się znaleźć, zachowując swoistą higienę (nie dotykamy i nie ściągamy wszystkiego „jak leci") i traktując innych internautów tak jak sami chcielibyśmy być traktowani. Internet stanowi medium, w którym znajdziemy wiele pozytywów. Internet pozwala nam na szybsze załatwienie rozmaitych codziennych spraw, jak np. płatności za rachunki, rozliczenia, zakupy, rezerwacje wakacyjnych wojaży i noclegów. Listę można by ciągnąć niemal w nieskończoność, ale dodam jeszcze tylko jeden istotny aspekt – a mianowicie technologie ułatwiają nam pozostawanie w kontakcie z ważnymi dla nas, najczęściej bliskimi nam, osobami. A dzięki kryptografii możemy to robić niemal pewni, że treści, które wymieniamy, mogą pozostać między nami (no i może niektórymi służbami lub operatorami naszych skrzynek pocztowych, jeśli godzimy się na utratę części prywatności, korzystając z ich usług).

Korzystajmy z technologii w dobrych celach i przeciwstawiajmy się agresji oraz próbom zawłaszczania naszego wirtualnego i rzeczywistego świata przez przestępców czy innych agresorów.

BEZPIECZEŃSTWO PRZED WOLNOŚCIĄ? PRÓBA ODPOWIEDZI W ŚWIETLE KLASYCZNEJ KONCEPCJI CZŁOWIEKA

KRZYSZTOF STACHEWICZ

Wydział Teologiczny UAM

TYTUŁEM WPROWADZENIA

W wolność człowieka są immanentnie wpisane rozliczne paradoksy, ujawniające z jednej strony jej złożoną naturę, a z drugiej trudności, jakie napotyka w życiu tak indywidualnym, jak i społecznym. Wydaje się, że jednym z pól, na których pojawia się struktura paradoksu, jest współistnienie wolności z bezpieczeństwem. Zapewnianie obywatelom bezpieczeństwa, zarówno zewnętrznego, jak i wewnętrznego, zawsze było i jest związane z ograniczaniem ich wolności i swobód, a poszerzanie tych drugich zdaje się ograniczać możliwości zapewniania bezpieczeństwa. To dylemat nienowy, można powiedzieć, że równie stary jak ludzka cywilizacja. Owszem, ostatnimi czasy, na skutek rozwoju techniki problem ten staje w nowym świetle i zdaje się nabierać szczególnie ekstremalnych postaci. „Za zapewnienie bezpieczeństwa odpowiadają dziś, jak się zdaje, przede wszystkim nowe technologie i techniki inwigilacji, które mają nas chronić nie tyle przed konkretnymi niebezpieczeństwami, ile raczej przed dość mglistymi i amorficznymi zagrożeniami”[1]. Powstaje zatem pytanie, czy ograniczanie wolności człowieka w imię chyba coraz bardziej

[1] Z. Bauman, D. Lyon, *Płynna inwigilacja. Rozmowy*, tłum. T. Kunz, Kraków 2013, s. 144. Por. D. Lyon, *Surveillance Studies: A. Overview*, Cambridge 2007.

mglistych i amorficznych – choć obrazowanych konkretami – zagrożeń jest antropologicznie i etycznie zasadne. A może bezpieczeństwo jest wyższym dobrem człowieka niż wolność? Stąd próba namysłu nad zakorzenieniem wolności i bezpieczeństwa w filozoficznej wizji człowieka i próba ich hierarchizacji. Mówiąc językiem filozofii człowieka Karola Wojtyły: „Chodzi mianowicie o sięgnięcie do tych podstaw, jakie tkwią w osobie"[2].

W tytule referatu i jego analizach przywołana zostaje klasyczna koncepcja człowieka. Kilka słów trzeba poświęcić temu określeniu. Władysław Tatarkiewicz wyróżniał cztery sensy terminu „klasyczność": to, co jest najlepsze, doskonałe, wzorcowe; to, co ma pochodzenie starożytne; to, co odpowiada wzorcom starożytnym, co udanie je wciela, oraz to, co posiada szczególne własności, jak harmonię, miarę i równowagę[3]. Pierwsze znaczenie terminu jest wyraźnie oceniające, trzy kolejne mają charakter opisowy. W odniesieniu do filozofii sens pierwszy wskazuje na doskonałość dzieł filozoficznych, drugi na jej starożytność, trzeci na powrót do starożytności. Najważniejszy jednak zdaje się być sens czwarty, który swe wcielenie uzyskał w dziełach Platona i Arystotelesa oraz tych kierunków filozoficznych, które nawiązywały do wielkich intuicji metafizycznych tych myślicieli. Maksymalizm, realizm, ostatecznościowy sposób wyjaśniania oraz autonomia metodologiczna w odniesieniu do innych typów wiedzy zdaje się stanowić demarkację klasycznego filozofowania w stosunku do jego wariantów nieklasycznych[4]. Chyba najbardziej zbliżony do tego ideał myśli klasycznej jest zawarty w dziełach Arystotelesa i filozofów do niego wprost nawiązujących, by wspomnieć św. Tomasza z Akwinu. Oprócz filozofii perypatetyckiej do klasycznych koncepcji włączyć należy te typy filozofii nowożytnej i współczesnej, które są maksymalistyczne, tzn. metafizyczne, wbrew rozmaitym tendencjom epok oraz czasów, i które podejmują zawsze aktualne, a postawione w dalekiej starożytności pytania filozoficzne. Prawdziwie klasyczna filozofia zawiera w sobie określoną filozofię bytu i włączoną w całościową wizję rzeczywistości filozofię człowieka[5]. W tym właśnie obszarze myśli

[2] K. Wojtyła, *Osoba i czyn*, Kraków 1985, s. 333.

[3] W. Tatarkiewicz, *Czworakie rozumienie klasyczności*, „Ethos" 1996, 35–36, s. 69–71. W odniesieniu do dzieł sztuki pisał autor tak: „Klasyczny w sensie A oznacza wartość dzieła, w sensie B określa czas jego powstania, w sensie C jest nazwą stylu historycznego, w sensie D – kategorii estetycznej" (s. 71).

[4] Por. A. Bronk, S. Majdański, *Klasyczność filozofii*, „Ethos" 1996, 35–36, s. 134.

[5] *Filozofia klasyczna to filozofia metafizyczna. Z profesorem Stefanem Swieżawskim rozmawia*

filozoficznej chcemy przyjrzeć się tytułowemu problemowi. Zabieg ten ma przeciwdziałać kakofonicznym klimatom myśli współczesnej o człowieku, a opiera się na zaufaniu do intuicji klasycznych myślicieli, którzy ciągle mają nam wiele do powiedzenia na temat człowieka. Mam wrażenie, że dużo więcej, ciekawiej i celniej niż modne dziś wizje antropologiczne rozwijane przez sezonowych myślicieli.

W kontekście rozpatrywanego w tekście problemu ujawnia się też silnie z nim związane pytanie o prywatność człowieka w świecie późnej nowoczesności. Zagadnienie prywatności i pytanie o jej granice zawsze stanowiło ważny problem antropologiczno-etyczny oraz społeczny. Ogólnie możemy określić prywatność jako wolność od prób nieautoryzowanego przez człowieka dostępu. Dziś, w dobie cyfrowej, problem polega na tym, że wiele naruszeń prywatności dokonuje się przy naszej nieświadomej najczęściej „autoryzacji" poprzez akceptację „formułek napisanych drobnym drukiem"[6]. W jednej z książek podejmujących problem inwigilacji czytamy: „Żyjemy w społeczeństwie nadzorowanym – w świecie masowego śledzenia, w którym instytucje gromadzą dane o jednostkach w niespotykanym dotąd tempie"[7]. Idea społeczeństwa nadzorowanego, o którym mówił Michel Foucault, zrealizowała się w stopniu, o którym nie myślał francuski strukturalista. W kontekście dzisiejszych technik inwigilacji z uśmiechem czytamy o wynalazkach technicznych umożliwiających podglądanie cudzego życia, o których pisała pół wieku temu Maria Ossowska: „podsłuch, magnetofon, teleobiektyw, szyby jednostronnie przezroczyste, fotografie bez wiedzy fotografowanego, aparaty do sprawdzania czyjejś prawdomówności, czyli tzw. poligrafy"[8]. Ciągi dalsze tej wynalazczości osiągnęły przez kolejne półwiecze nieprzewidywalne wtedy rozmiary. Generalnie możemy inwigilację uznać za charakterystyczną cechę nowoczesnego świata, która w czasach późnej nowoczesności zdaje się zmierzać

---

ks. Jarosław Merecki, „Ethos" 1996, 35–36, s. 255. Czytamy: „nie ma prawdziwej filozofii bez filozofii bytu i bez filozofii człowieka" (s. 260).

[6] Por. J. Angwin, *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, Warszawa 2017, s. 20. Por. N. Postman, *Technopol. Triumf techniki nad kulturą*, tłum. A. Tanalska-Dulęba, Warszawa 1995.

[7] J. Angwin, *Społeczeństwo nadzorowane,* s. 20. Simon Borel zauważa, że człowiek permanentnie działający w sieci staje się „własnym despotą, kiedy udostępnia z własnej nieprzymuszonej woli niezliczone ilości danych osobowych, z których korzystają cyfrowi giganci i państwa" (cyt. za: J.-H. Lorenzi, M. Berrrebi, *Przyszłość naszej wolności. Czy należy rozmontować google'a i kilku innych?*, tłum. J. Nowakowska, Warszawa 2019, s. 146).

[8] M. Ossowska, *Normy moralne. Próba systematyzacji*, Warszawa 1985, s. 101.

ku jakiemuś apogeum pod hasłami wymogów bezpieczeństwa[9]. Określenie Deleuze'a „społeczeństwo kontroli" robi dużą karierę jako kategoria opisująca współczesność. Gromadzenie danych klientów przez wielkie firmy, handel wielkimi zbiorami danych („big data") w myśl zasady, że dane to waluta cyfrowego świata, profilowanie klientów czy nieustanne śledzenie w sieci – przez rządy, korporacje i jednostki[10] – stawia w nowym świetle pytanie, jak w tym kontekście ma się prywatność, przestrzeń tego, co stanowi mój świat, w którym ja podejmuję decyzję i kształtuję swe życie i swą egzystencjalną przestrzeń? Bill Binney, były wysoki funkcjonariusz wywiadu Agencji Bezpieczeństwa Narodowego USA, ostrzega, że ilość danych gromadzonych przez NSA przekracza o całe rzędy wielkości to, co pozyskały najbardziej opresyjne reżimy tajnej policji, jak choćby Gestapo, Stasi czy KGB: „Gromadzenie przez rząd tak wielkich ilości informacji o obywatelach stanowi dla nas prawdziwe zagrożenie. Daje mu władzę nad każdym z nas"[11].

Ossowska w *Normach moralnych* wyróżniła trzy podstawowe sensy prywatności. Po pierwsze, jest to prawo do tymczasowej samotności, przeciwstawienie się stadności życia; po drugie, jest to wolność od obcej kontroli, przynajmniej we własnym domu, i po trzecie, prawo do obrony przed ciekawością ludzką, niechcianą poufałością, niedyskrecją[12]. Najbardziej interesujący z naszego punktu widzenia jest sens drugi, wyraźnie nawiązujący do wolności i bezpieczeństwa. To tu właśnie ingerencja w prywatność uderza w ludzką wolność, ale i bezpieczeństwo, i tym samym generuje jakąś fundamentalną postać antropologicznego zła. Prywatność wiąże się bowiem ściśle z autodeterminacją, decydowaniem o sobie, określonym – mówiąc frazą Kierkegaarda – „poczynaniem samego siebie". Związek z wolnością jest tu zatem oczywisty, a wszelkie formy inwigilacji stanowią jakąś formę jej naruszania. Ale i poczucie bezpieczeństwa jest naruszone w przypadku zewnętrznej kontroli, nadzoru, wykorzystywania władzy. „Ten brak poczucia bezpieczeństwa we własnym domu dał nam się we znaki w czasie okupacji niemieckiej, kiedy to odgłos ciężkich butów na schodach zapierał oddech

[9] Por. Z. Bauman, D. Lyon, *Płynna inwigilacja*…, s. 9: „Inwigilacja jest kluczowym wymiarem nowoczesnego świata i w większości krajów ludzie doskonale zdają sobie sprawę, jak duży wpływ wywiera ona na ich życie". I dalej: „Istnieje powszechna zgoda co do tego, że inwigilacja jest podstawowym wymiarem nowoczesności" (s. 11).

[10] J. Angwin, *Społeczeństwo nadzorowane*…, s. 66 nn.

[11] Tamże, s. 72.

[12] Por. M. Ossowska, *Normy moralne*…, s. 102–106.

w trwożnym oczekiwaniu”[13]. Pewne formy zaprowadzania ładu i porządku, mających zapewnić bezpieczeństwo, gruntownie poczucia bezpieczeństwa pozbawiają. Ale i w trzecim sensie jawi się zagrożenie dla naszej godności oraz praw wolności i bezpieczeństwa. Wszak gromadzenie danych o kimś, znajomość cudzego życia bez zgody zainteresowanego (czy przy jego nieświadomej konsekwencji zgodzie) może być użyte dla celów związanych z realizacją władzy nad człowiekiem, manipulowania nim i jego potrzebami, a tym samym godzić w jego wolne wybory.

Pytając w kontekście klasycznego obrazu człowieka o miejsce wolności i bezpieczeństwa w hierarchii dóbr osoby ludzkiej, musimy wstępnie zarejestrować ogromną dysproporcję między filozoficznymi analizami wolności i bezpieczeństwa. Filozofia wolności to jedna z najbardziej rozbudowanych części klasycznej antropologii filozoficznej, natomiast bezpieczeństwo ma nie tylko ubogą reprezentację, ale generalnie trzeba jej poszukiwać w różnych przebraniach słownych. Granice prywatności i indywidualności jawią się jako zaniedbany problem filozofii społecznej. Sekurologia filozoficzna czeka na swe opracowanie, gdyż próżno by szukać w klasycznych tekstach filozoficznych jej w miarę pełnej eksplikacji problemowej[14]. Powody tego stanu rzeczy, mam nadzieję, przynajmniej częściowo ujawnią się w naszych analizach.

Czy poczucie bezpieczeństwa jest warunkiem realizowania wolności? Czy też stwarzanie warunków dla poczucia bezpieczeństwa z istoty swej pociąga za sobą ograniczanie wolności, kurczenie się przestrzeni wolnego wyboru i decydowania o kształcie swych działań, poczynania samego siebie w wolności, bycia sobą w przestrzeni prywatności? Czy implikacje normatywne płynące z wartości bezpieczeństwa z istoty swej są nastawione na to, by nie zagrażać innym fundamentalnym dla życia człowieka wartościom? Czy raczej obie wartości są wzajemnie ze sobą sprzężone i wzajemnie się zakładają?[15] Te i inne pytania będą wyznaczały kierunki naszych dalszych refleksji.

---

[13] Tamże, s. 103.

[14] Por. J. Szmyd, *Poczucie bezpieczeństwa jako wartość społeczna, etyczna i egzystencjalna. Rozważania podstawowe*, „Państwo i Społeczeństwo” 2014, 2, s. 12–19. Por. też: A. Gdula, *O bezpieczeństwie człowieka jako wartości*, „Doctrina. Studia społeczno-polityczne” 2010, 7, s. 45–50.

[15] „Bezpieczeństwo bez wolności równa się niewolnictwu” – zauważa Bauman, ale zaraz dodaje: „wolność bez bezpieczeństwa oznacza dręczące poczucie porzucenia i zagubienia” (Z. Bauman, *Wspólnota. W poszukiwaniu bezpieczeństwa w niepewnym świecie*, tłum. J. Margański, Kraków 2008, s. 30–31).

HOMO LIBERALIS – W POSZUKIWANIU WOLNOŚCI CZŁOWIEKA

U progu średniowiecza Boecjusz, zamykający poniekąd epokę starożytną, sformułował określenie człowieka, które stało się klasyczną jego definicją: *naturae rationalis individua substantia* (substancja indywidualna mająca rozumną naturę). Indywidualność stała się nerwem określenia osoby ludzkiej, tworząc naturalne niejako napięcie między tym, co jednostkowe, a tym, co wspólnotowe. Starożytność generalnie radziła sobie z tym napięciem, marginalizując jednostkowość na rzecz wspólnoty, polis, pewnej całości, w którą wpisuje się niemal bez reszty człowiek. Wydobycie i silne zaakcentowanie jednostkowości w myśli chrześcijańskiej postawiło to napięcie w całej ostrości. To myśl chrześcijańska – jesteśmy tu w zgodzie ze stanowiskiem Hannah Arendt[16] – wprowadziła do filozofii europejskiej rozumienie indywidualnej wolności w postaci wolnej woli, by wskazać tylko na pisma św. Augustyna i jego koncepcję *liberum arbitrium*. Wcześniej pojęcie to, mówiąc nieco kolokwialnym skrótem, nie było potrzebne dla analizy rzeczywistości ludzkiej. Czym zatem jest wolność i związana z nią wolna wola? Chęć choćby skrótowego zarysowania dziejów tego pojęcia w filozofii trzeba potraktować jako pokusę, którą trzeba zwalczyć. Zgodnie z precyzacją w tytule referatu skupimy się na myśli klasycznej, ze szczególnym uwzględnieniem konkretnej koncepcji wolności.

Tomasz z Akwinu analizował mechanizm wolnego wyboru przede wszystkim w swej monumentalnej *Sumie teologicznej* I-II, kwestie 12–15. Wskazywał, że wolność jest wyborem jednej z wielu możliwości, za czym stoi fakt, że jedną rzecz stawiamy wyżej od innej. Rozum nazywał Akwinata „korzeniem wszelkiej wolności". W filozofii perypatetycko-tomistycznej generalnie wychodzi się od rejestracji powszechnego fenomenu świadomości działania wolnego, nieprzymuszonego. Mieczysław A. Krąpiec zauważał: „działając, wiemy o tym, że możemy wykonywać to właśnie działanie, że nie jesteśmy przymuszeni do wykonywania tego działania. Doświadczamy, że chcemy tak właśnie działać"[17]. Poznanie to nie ma charakteru abstrakcyjnego, nie jest

[16] Por. H. Arendt, *Wola*, tłum. R. Piłat, Warszawa 1996, s. 126–159. Por. O. Patterson, *Wolność, niewolnictwo i nowoczesna konstrukcja uprawnień*, tłum. M. Bucholc, M. Kaczmarczyk, [w:] *Kulturowe wartości Europy*, red. H. Joas, K. Wiegandt, Warszawa 2012, s. 137–138.

[17] M.A. Krąpiec, *Natura ludzkiej wolności*, [w:] *Wolność we współczesnej kulturze*, red. zb., Lublin 1997, s. 32. Szerzej o wolności pisał Krąpiec w monografii pt. *Ja człowiek. Zarys antropologii filozoficznej*, Lublin 1986, s. 217–256.

poznaniem przedmiotowym, jest refleksją stale towarzyszącą naszemu działaniu, refleksją *in actu exercito*, a nie *in actu signato*, by użyć klasycznego rozróżnienia wypracowanego w scholastyce. „I właśnie refleksja towarzysząca jest autentycznym świadkiem wolności naszych aktów decyzyjnych, a przez to samo naszej ludzkiej wolności”[18]. Ten powszechny fenomen, płynący ze świadomości wolności w działaniu, domaga się filozoficznego wyjaśnienia. Wolność rozumie się jako niezależność od przymusu, skrępowania („wolność od”), stąd dzieli się ją na wolność zewnętrzną (niezależność od przymusu zewnętrznego wobec człowieka) i wolność wewnętrzną (niezależność od przymusów wewnętrznych; wolność wyboru). Tradycyjna antropologia tomistyczna mówiła o trzech rodzajach wolności wewnętrznej: wolność działania (*libertas exercitii*) polega na wyborze między podjęciem czynności lub jej zaniechaniem, wolność ugatunkowienia (*libertas specificationis*) – swoboda wyboru między czynnościami i przedmiotami gatunkowo różnymi, i wolność przeciwieństwa (*libertas contrarietatis*) jako swoboda wyboru między przedmiotami i czynnościami przeciwnymi[19].

Wolność jawi się jako wspólny fenomen działania rozumu i woli, gdyż ujawnia się ona w aktach decyzyjnych, zakładających poznanie z jednej strony, a chcenie z drugiej. Jak zauważał św. Tomasz: „Na wybór zaś składa się coś z władzy poznawczej i coś z władzy pożądawczej” (STh I, q. 83, a.3c). Wolność człowieka „wypowiada się” w aktach decyzyjnych, następujących po namyśle, a poprzedzających wykonanie: „Na ludzką decyzję, czyli ludzki wolny wybór będący źródłem działania człowieka, składają się czynności poznania intelektualnego i aktu wolnego wyboru dokonanego przez naszą wolę”[20]. Wola jest zawsze nastawiona na wybór dobra, nigdy zła jako takiego. Oba akty, tzn. rozumu i woli, wzajemnie się przeplatają, pozostają – jak mówił Krąpiec – w „dialektycznym spięciu”, konstytuując jeden akt decyzji. Intelekt wskazuje w określonym sądzie praktycznym określone treści, a wola odpowiada aktem przyzwolenia, wyboru, zgodnie z adagium: *nihil volitum, nisi praecognitum*. Przy czym wola wybiera nie dobro, lecz określony sąd praktyczny o określonym dobru[21]. Dobro jest na zewnątrz mnie, stąd nie mogę go wybrać bezpośrednio, jest ono zawsze poniekąd zapośredniczone przez praktyczny sąd o dobru. Co jest zatem ostatecznym uzasadnieniem wolności? Krąpiec pisał: „Jest nią

[18] M.A. Krąpiec, *Natura ludzkiej wolności*…, s. 32.
[19] Por. np. G. Dogiel, *Antropologia filozoficzna*, Kraków 1984, s. 43.
[20] M.A. Krąpiec, *Natura ludzkiej wolności*…, s. 36.
[21] Por. tamże, s. 37.

nasza bytowa struktura, wyrażająca się ostatecznie w samej naturze intelektu i woli"[22]. Bez wolności nie ma ludzkiej natury w działaniu, znika podmiot czynu: „Tylko bowiem w akcie decyzyjnym człowiek wypowiada się jako człowiek"[23]. Wyłącznie w wolności i poprzez wolność człowiek tworzy swe własne oblicze, kreuje kształt swego indywidualnego człowieczeństwa, tylko poprzez wolność człowiek staje się odpowiedzialny za siebie samego, za innych ludzi, w jakimś sensie za rzeczywistość. Stąd można powiedzieć, że „świat człowieka to świat wolności"[24].

Wyróżnia się często takie typy wolności, jak: wolność polityczna, społeczna, ekonomiczna, artystyczna, wolność słowa, sumienia, wyznania, opinii, własności, myśli, uczuć, co wyraźnie wskazuje na wzajemne przyporządkowanie do siebie wolności i indywidualności osoby ludzkiej. Już to wprowadza napięcie wynikające z rozróżnienia prywatne – wspólnotowe/społeczne, choćby w aspekcie relacji wolności i prawa, które niejako z istoty ogranicza spontaniczną wolność indywiduów. U Hegla mamy wizję państwa jako wolności[25]. Absolutyzował on państwo i tworzone przez nie prawo. Procesy uzyskiwania przestrzeni wolności przez grupy społeczne czy poszczególnych ludzi określa się mianem procesów emancypacyjnych.

Mówiąc o fundamentalnych typach wolności, Erich Fromm wyróżniał wolność „od", jako niezależność człowieka od determinizmów, i wolność „do", jako możliwość afirmacji ideałów, wewnętrzny rozwój człowieka. Isaiah Berlin pisał o wolności „negatywnej" (brak ingerencji w naszą

---

[22] Tamże, s. 38.

[23] Tamże, s. 39.

[24] S. Kowalczyk, *Kim jest człowiek? Elementy antropologii*, Wrocław 1992, s. 67. Por. S. Kowalczyk, *Podstawy światopoglądu chrześcijańskiego*, Warszawa 1980, s. 70–85. Czytamy: „Jedną z fundamentalnych wartości człowieka jest wolność. Ona specyfikuje ludzki byt, jest jego trwałym fundamentem i sensem. Kosmos bez wolności człowieka nie miałby inicjatywy, własnych celów i racji istnienia. Ludzkie życie posiada sens, ponieważ człowiek jako istota myśląca jest zdolny do wolnego działania i samokierowania" (s. 70). I dalej: „Być człowiekiem to znaczy być wolnym" (s. 72). Por. S. Kowalczyk, *Człowiek a społeczność. Zarys filozofii społecznej*, Lublin 1994, s. 162–179. „Wolność należy do istoty bytu ludzkiego: jest jego sercem, azylem, źródłem wartości. Bez wolności życie ludzkie, w przekonaniu wielu, traci sens. Wolność sprawia, że człowiek jest osobą i podmiotem, autorem swej biografii w jej wymiarze indywidualnym i społecznym" (s. 162). „Wolność to misterium osoby ludzkiej" (s. 170). Erich Fromm zauważał, że „wolność jest specyficzną cechą ludzkiej egzystencji jako takiej – i dalej – że jej znaczenie zmienia się zależnie od stopnia świadomości człowieka i pojęcia o sobie samym jako bycie niezależnym i wyodrębnionym" (E. Fromm, *Ucieczka od wolności*, tłum. O. i A. Ziemilscy, Warszawa 1970, s. 42).

[25] G.W.F. Hegel, *Wykłady z filozofii dziejów*, t. 1, tłum. J. Grabowski, A. Landman, Warszawa 1958, s. 70.

działalność) i „pozytywnej" (pragnienie bycia panem swego losu)[26]. Bogata retoryka czasów współczesnych wysławiająca wolność zdaje się jednak skrywać niebezpieczne trendy. Marian Golka tak pisze: „W imię dążenia ludzi do wolności i niezależności cywilizacja zachodnia stworzyła niezwykle atrakcyjne, wygodne, a przy tym nader opresyjne środki, które dając złudzenie wolności i niezależności, w istocie są nowym sposobem zniewolenia"[27]. Nawet jeśli to opis przesadzony, to jednak trudno go *en bloc* zakwestionować.

EKSKURS I. SAMOSTANOWIENIE JAKO WYRAZ WOLNOŚCI: WOKÓŁ FILOZOFII WOLNOŚCI KAROLA WOJTYŁY

W tym roku mija 50 lat od pierwszego wydania dzieła Karola Wojtyły pt. *Osoba i czyn*. To niezwykle interesująca i inspirująca monografia, która – w mojej ocenie – ciągle nie doczekała się adekwatnej odpowiedzi ze strony polskiej filozofii. Znajdziemy w niej interesującą koncepcję wolności, którą poniżej krótko omówię. To przykład współczesnego myślenia o wolności w kontekście klasycznej filozofii człowieka. Stąd chcemy w osobnym paragrafie przyjrzeć się Wojtylańskim intuicjom filozoficznym dotyczącym ludzkiej wolności.

Wolność ujawnia nam się w przeżyciu, które Karol Wojtyła określa krótko: „mogę – nie muszę". To nie tylko treść świadomości, ale i przejaw właściwego człowiekowi dynamizmu. Między tymi biegunami: „mogę" i „nie muszę" rodzi się człowiecze „chcę", jako zdynamizowanie woli, owej władzy ludzkich wyborów, chcenia właśnie. Wolność jawi się z jednej strony jako moment decydujący o sprawczości człowieka (wszak nie mogę czuć się sprawcą czegoś, co leży poza moją wolnością), a z drugiej jest elementem konstytuującym strukturę „człowiek działa" w jej odrębności od wszystkiego, co dzieje się w człowieku („bierność). Wojtyła, analizując powyższe kwestie, dochodzi do odkrycia struktury samostanowienia, charakterystycznej dla bytu człowieka. „Samostanowienie stanowi istotę wolności człowieka"[28]. Można powiedzieć,

[26] Por. I. Berlin, *Dwie koncepcje wolności i inne eseje*, tłum. zb., Warszawa 1991, s. 113–134.
[27] M. Golka, *Paradoksy wolności*, Warszawa 2017, s. 85.
[28] K. Wojtyła, *Osobowa struktura samostanowienia*, [w:] tenże, *Osoba i czyn…*, s. 426–427. Por. A. Szostek, *Wolność jako samostanowienie. Karola Wojtyły koncepcja wolności*, [w:] *Wolność we współczesnej kulturze*, s. 442–445.

że samostanowienie to doświadczalnie dana struktura ludzkiej wolności. Fundamentem samostanowienia jest samo-posiadanie. Nie można wszak dokonywać aktów samostanowienia bez samo-posiadania: „Stanowić bowiem można tylko o tym, co się realnie posiada"[29]. Wskazuje to na doniosłą kwestię: „Osoba jest mianowicie tym, kto siebie samego posiada, i zarazem tym, kto jest posiadany tylko i wyłącznie przez siebie"[30]. Scholastyka wyrażała to w zdaniu: „*persona est sui iuris*". Wojtyła odsłania w swych analizach jeszcze jeden moment, konieczny dla funkcjonowania struktury samostanowienia, mianowicie samo-panowanie, gdzie osoba sama sobie panuje. „Raczej więc wypada tu mówić o «panowaniu sobie»" niż o «panowaniu nad sobą»"[31]. W aktach samostanowienia ujawnia się natura osoby ludzkiej, wskazując, że człowiek panuje samemu sobie i wykonuje wobec siebie tę fundamentalną władzę, której nikt za niego sprawować nie może. Samostanowienie jako przymiot osoby to właśnie wolność. Wolność to przymiot woli człowieka, to efekt zależności od własnego „ja". Poza przestrzenią tej zależności mamy przestrzeń konieczności, w której nie może być mowy o samostanowieniu, sprawczości. Warto zwrócić uwagę na ten moment „zależności", który jest w omawianej koncepcji kluczowy. Wszak najczęściej rozumie się wolność właśnie poza wszelkimi zależnościami. To interesujący trop myślowy Wojtyły, godny wszechstronnego rozwijania. Charakterystyczne w tym właśnie kontekście jest to, że Wojtyła rzadko posługuje się kategorią pojęciową „wolność", uwikłaną wszak w niezliczoną ilość presupozycji teoretycznych, używając najczęściej pojęcia „samostanowienie", które wyprowadził z doświadczalnego oglądu człowieka w jego sprawczości.

Człowiek transcenduje swą podmiotowość w intencjonalności, przekraczając granicę między podmiotowością a przedmiotowością (transcendencja pozioma). Wojtyła zwraca jednak uwagę przede wszystkim na transcendencję osoby w czynie, dokonującą się dzięki samostanowieniu (transcendencja pionowa). Tu ujawnia się wspomniana zależność od własnego „ja" (samozależność), jego nadrzędność. Wojtyła pisał: „Człowiek jest wolny – to znaczy, że w dynamizowaniu swego podmiotu zależy sam od siebie"[32]. Wolność zakłada zatem stanowienie przez byt ludzki konkretnego, indywidualnego „ja" – tylko wtedy podmiot staje się dla samego siebie przedmiotem, tworząc strukturę „uprzedmiotowienia", stanowiącą

[29] K. Wojtyła, *Osoba i czyn* …, s. 152.
[30] Tamże.
[31] Tamże, s. 153.
[32] K. Wojtyła, *Osoba i czyn*…, s. 165.

conditio sine qua non wolności: „Uprzedmiotowienie mianowicie warunkuje samozależność, w której zawiera się podstawowe znaczenie wolności”[33]. Autor *Osoby i czynu* podkreślał, że istnieje ścisła proporcjonalność między stopniem świadomości działania i świadomości wartości realizowanej w czynie a stopniem przeżywania samostanowienia. A „im wyraźniej [człowiek – K.S.] przeżywa samostanowienie, tym jaśniej w przeżyciu i świadomości rysuje się własna sprawczość i odpowiedzialność”[34]. Tym bardziej działam jako człowiek, angażując swoją najgłębszą istotę.

Samostanowienie Wojtyła rozumie w kontekście posługiwania się wolą przez osobę ludzką, jako właśnie autodeterminację. Wola ujawnia zatem obok momentu bytowego człowieka także aspekt władzy. Czytamy: „Wolą wszakże nazywamy nie tylko to, co ujawnia, a zarazem aktualizuje strukturę samo-posiadania oraz samo-panowania, ale także i to, czym człowiek posługuje się, czego poniekąd używa do osiągnięcia swoich celów”[35]. Wola więc nie tyle stanowi o osobie, ale przede wszystkim zależy od osoby, jest przeto od niej różna i niższa. Osoba posiada wobec woli pozycję radykalnie nadrzędną, co wyraża formuła: „mogę chcieć – lub nie chcieć”, co wyraźnie ujawnia władzę osoby nad wolą. Wola jawi się jako „władza wolności osoby”[36], „centralna władza duszy ludzkiej”[37], w której aktualizuje się struktura samostanowienia. Człowiek posługuje się wolą, realizując samostanowienie, będąc sprawcą czynu, dokonując fundamentalnego aktu autodeterminacji. Człowiek dynamizuje się jako osoba poprzez wolność, a jej przejawem jest właśnie władza woli. Wojtyła posługuje się wręcz określeniem „instynkt wolności”, chcąc podkreślić, że wolność jest naturalnym środowiskiem czynów człowieka, wyrastających z podstawowej struktury samostanowienia (świadome rozstrzyganie). W sposób chyba najpełniejszy wolność ujawnia się w człowieku w jego zdolności wybierania, co zakłada jakąś niezależność od przedmiotów w porządku intencjonalnym. Oczywiście, nie ma tu mowy o braku uwarunkowań przez przedmioty czy wartości. „Nie jest to bowiem wolność od przedmiotów, od wartości, lecz wręcz przeciwnie – wolność do nich albo lepiej jeszcze się wyrażając – wolność dla nich: dla przedmiotów, dla wartości”[38]. Ten moment „do”, „dla” wpisany w dynamizm ludzkiej wolności jest w omawianej koncepcji bardzo ważny.

---

[33] Tamże.
[34] K. Wojtyła, *Osobowa struktura samostanowienia*, [w:] tenże, *Osoba i czyn…*, s. 426.
[35] K. Wojtyła, *Osoba i czyn…*, s. 167.
[36] Por. tamże.
[37] K. Wojtyła, *Osobowa struktura samostanowienia*, [w:] tenże, *Osoba i czyn…*, s. 426.
[38] K. Wojtyła, *Osoba i czyn…*, s. 177.

Spełnianie się siebie w czynie jest ściśle związane ze szczęściem, co uwyraźniało się już w myśli Arystotelesa, choćby w *Etyce nikomachejskiej*. Wojtyła zauważał: „Pola szczęśliwości należy szukać w tym, co wewnętrzne i nieprzechodnie w czynie – co utożsamia się ze spełnieniem siebie jako osoby”[39]. Prawda i wolność, wzajemnie ze sobą powiązane, stanowią fundament tak rozumianej szczęśliwości. Tylko zespolenie wolności z prawdą tworzy środowisko, w którym człowiek może spełniać siebie jako osobę ludzką, a tym samym stawać się szczęśliwym (eudajmonizm). Sama wolność nie jest jeszcze sama w sobie szczęściorodna, stanowiąc wyłącznie warunek osiągnięcia szczęścia. Dopiero wolność spełniająca się przez prawdę prowadzi do szczęścia. Już w samym słowie „samostanowienie” jest zawarty moment jakiejś kreacji siebie, stanowienia o sobie: „człowiek nie tylko jest sprawcą swoich czynów, ale przez te czyny jest zarazem w jakiś sposób «twórcą siebie samego»”[40]. Wybór konkretnej wartości określa zarazem samego człowieka, który staje się w tym wyborze i przez niego człowiekiem dobrym lub złym. „Człowiek stanowi nie tylko o swoim działaniu, ale także stanowi o sobie w aspekcie najbardziej istotnej jakości. W ten sposób samostanowieniu odpowiada stawanie się człowieka jako człowieka”[41]. Henri Bergson, mówiąc o wolności, używał dobrze współbrzmiącej z powyższymi analizami frazy: „branie w posiadanie siebie”[42].

Wszystko to uzasadnia centralną pozycję struktury samostanowienia w ontologii osoby ludzkiej, pozycję, którą przypisywał samostanowieniu Wojtyła. To dzięki niemu i przez nie człowiek może pomnażać dobro w świecie, a jednocześnie sam stawać się dobrym. Bardziej newralgicznego momentu w ontologii osoby ludzkiej raczej wskazać się nie da. Wolność jest immanentnie wpisana w strukturę osoby ludzkiej, stąd można zasadnie powiedzieć, że wolność jest naturą człowieka.

CZŁOWIEK W POSZUKIWANIU BEZPIECZEŃSTWA

Bezpieczeństwo to, słownikowo, stan niezagrożenia, spokoju, pewności, jakiegoś ładu, porządku, który niweluje potencjalne lęki i strachy. Z psychologicznego punktu widzenia potrzeba bezpieczeństwa jako swoiste

[39] Tamże, s. 217.
[40] K. Wojtyła, *Osobowa struktura samostanowienia…*, s. 428.
[41] Tamże, s. 428.
[42] Por. H. Bergson, *Ewolucja twórcza*, tłum. F. Znaniecki, Warszawa 1957, s. 139.

pragnienie trwania, spokoju, stabilizacji, jawi się jako jedna z najbardziej fundamentalnych potrzeb człowieka. Pisał Stefan Garczyński: „Potrzeba bezpieczeństwa, będąc w swoich najprostszych postaciach wyrazem instynktu samozachowawczego, jest potrzebą psychiczną najbliższą biologicznych”[43]. Harry Stack Sullivan wskazuje, że potrzeba bezpieczeństwa nie tylko pojawia się bardzo wcześnie w życiu dziecka, ale jest też znacznie ważniejsza niż impulsy płynące z głodu czy pragnienia[44]. Filozof jest poniekąd skazany na poszukiwanie bezpieczeństwa w takich obszarach analizy zjawisk, jak: życie, zdrowie, prywatność, godność, niezawisłość, a nawet przyjemności. Wskazuje się na różne aspekty bezpieczeństwa, skorelowane z poszczególnymi obszarami ludzkiego bytowania, mówiąc o bezpieczeństwie pozycji, finansów, fizycznym, psychicznym etc. W Tomaszowej koncepcji prawa naturalnego bezpieczeństwo będzie leżało na przedłużeniu pierwszej inklinacji naturalnej, mówiącej o dążeniu do zachowania swego bytu. Tym samym wpisuje się w mocny kanon moralnych zobowiązań człowieka wobec siebie, ale i wobec innych.

Potrzeba bezpieczeństwa jest oczywiście skorelowana w swej sile z poczuciem zagrożenia, szczególnie w sytuacjach kontaktu z tym, co inne, nowe, nierozpoznane. Władza państwowa różnego typu próbuje nierzadko podsycać stan zagrożenia, by usprawiedliwić wyjątkowe środki do zapewnienia bezpieczeństwa. Przykłady są tak oczywiste, że nie trzeba ich tu przywoływać. Zresztą wiele zjawisk współczesnego życia, jak choćby silne wstrząsy rynku pracy powodujące permanentną niepewność, skutecznie zakłóca poczucie bezpieczeństwa. Dążenie do stanu bezpieczeństwa całkowitego, zupełnego jest oczywiście nierealizowalne, człowiek „potrzeby bezpieczeństwa nigdy bez reszty zaspokoić nie zdoła”[45]. Zresztą chyba nie byłoby to pożądane.

Za sprawą Anthony Giddensa dużą popularnością cieszy się we współczesnych dyskursach pojęcie „bezpieczeństwa ontologicznego”. Oznacza ono poczucie trwania i porządku zdarzeń, w tym również zdarzeń wykraczających poza obszar bezpośredniego doświadczenia jednostki. Poczucie bezpieczeństwa ontologicznego jednostka zyskuje, idąc drogą różnego rodzaju przeżyć, kryzysów i zawirowań i wyrabiając w sobie nawyki interpretacyjno-praktyczne, „konwencje życia codziennego” („świadomość praktyczna”). Istotnym elementem w tak pojmo-

[43] S. Garczyński, *Potrzeby psychiczne. Niedosyt, zaspokojenie*, Warszawa 1972, s. 40.

[44] Por. A. Giddens, *Nowoczesność i tożsamość. „Ja” i społeczeństwo w epoce późnej nowoczesności*, tłum. A. Szulżycka, Warszawa 2012, s. 69–70.

[45] S. Garczyński, *Potrzeby psychiczne*…, s. 50; por. J. Szmyd, *Poczucie bezpieczeństwa jako*..., s. 19.

wanym bezpieczeństwie jest, zdaniem Giddensa, „ufność pokładana w egzystencjalnych punktach zaczepienia, w sensie emocjonalnym i w pewnym stopniu poznawczym, opiera się na nabytej we wczesnych doświadczeniach dziecka pewności co do tego, że na innych można polegać”[46]. Zagrożenia tej stabilizacji, zakłócenia bezpieczeństwa ontologicznego jest dla człowieka późnej nowoczesności istotnym problemem, wpisującym się w siatkę problemową, którą tu rozważamy.

Niektórzy próbują ściśle łączyć ze sobą obie wartości, jak choćby Monteskiusz, twierdzący, że wolność polityczna polega na bezpieczeństwie[47]. Hobbes natomiast ujmował bezpieczeństwo jako fundament wspólnototwórczych dążeń człowieka. Współczesne formy zaspokajania potrzeby bezpieczeństwa w przestrzeni publicznej posiadają swój rewers w postaci rozmaitych typów opresji, by wymienić konsumeryzm, obiecujący realizację wolności[48], czy mediokrację, uzależniającą od siebie i manipulującą informacjami. W odniesieniu do tej drugiej trudno się nie zgodzić z taką konstatacją: „Media próbują arbitralnie decydować o wszystkim: o polityce, o obyczajach, o systemie wartości”[49]. Dość skutecznie też zaciera się granica między tym, co prywatne, a tym, co publiczne. Dobrym przykładem jest Facebook, na którym z własnej woli nie tylko pozbywamy się anonimowości, ale czynimy publicznym to, co do niedawna stanowiło przestrzeń prywatności. Paradoksalnie brzmiące słowa współczesnego myśliciela zdają się trafiać w istotę sprawy: „Obecnie zatrważa nas nie tyle możliwość zdradzenia lub pogwałcenia prywatności, ile wizja przeciwna: zamkniętych dróg wyjścia ze sfery prywatności”[50].

Inwigilacja w czasach współczesnych daje niezwykle szerokie możliwości oraz przybiera charakterystyczne, a często złudne formy bezpieczeństwa. Nadzór przestaje kojarzyć się z więzieniem, a jego coraz bardziej lekka i elastyczna forma raczej wiąże się z rozrywką

---

[46] A. Giddens, *Nowoczesność i tożsamość*…, s. 61. Dalej czytamy: „Bezpieczeństwo ontologiczne na poziomie nieświadomości i świadomości praktycznej to tyle, co umiejętność udzielenia «odpowiedzi» na pytania egzystencjalne, które w taki czy inny sposób stawia samo ludzkie życie” (s. 73).

[47] Monteskiusz, *O duchu praw*, Warszawa 1957, t. 1, s. 276.

[48] Por. L. Hostyński, *Granice wolności w świecie konsumpcji*, [w:] *Wolność w epoce przemian*, red. M. Szulakiewicz, Z. Karpus, Toruń 2007, s. 57–64. Marian Golka pisze: „W istocie – konsumpcja pożera. Pożera osobowości ludzi, pożera sumienia, pożera ich zdrowie, ich czas a także, o dziwo, ich szczęście. Pożera harmonię społeczną. Pożera przyrodę. Pożera wolność. (…) daje jednocześnie poczucie bezpieczeństwa” (M. Golka, dz. cyt., s. 73).

[49] M. Golka, dz. cyt., s. 78.

[50] Z. Bauman, D. Lyon, *Płynna inwigilacja*…, s. 46.

czy konsumpcją, dając fałszywe poczucie wolności[51]. Trafnie zauważa Bauman: „O ile niegdyś należało przyjąć, że strażnik w *panoptikonie* był jednak (gdzieś) obecny, o tyle w dzisiejszym układzie władzy ci, którzy ją sprawują, mogą w każdej chwili rozpłynąć się w powietrzu – stać się niedostępni i nieosiągalni"[52]. Współczesny *panoptikon* wyzbył się topornych cech z pomysłów Benthama, natomiast pełniej realizuje jego ideę, by dać ludziom poczucie, że są pod stałym nadzorem, i kształtować ich wybory i decyzje. W Chinach na dwie osoby w 2020 roku ma przypadać jedna kamera. Oczywiście poza celami bezpieczeństwa realizowane będą cele polityczne w postaci choćby wyłuskiwania i namierzania dysydentów. Nowe technologie mają umożliwiać nie tylko rozpoznawanie twarzy (kamery biometryczne), ale też skanowanie i analizowanie stanów psychicznych człowieka. Zauważyć wypada, że niezależnie od tego, czy inwigilacja działa czy nie, już sama wiara ludzi w to, że ona funkcjonuje, wpływa korygująco na ich zachowania[53]. Liczba kamer w przestrzeni publicznej wzrasta wykładniczo także w krajach europejskich, by wspomnieć Wielką Brytanię, gdzie ich liczba dawno przekroczyła 4 mln. A świadomość, że *Big Brother is watching you* upowszechnia się coraz bardziej. Przy czym Wielki Brat spogląda z naszego smartfona, który dobrowolnie stał się towarzyszem naszej drogi i który rejestruje nasze rozmowy, aktywność w sieci. Sfera prywatności kurczy się do jakichś kuriozalnych rozmiarów, a wolność jest zastępowana kontrolą i coraz silniejszym wpływaniem na określony sposób zachowania. Przy czym współczesna akceptacja kontroli społecznej zaspokaja nie tylko, a może nie przede wszystkim, potrzebę bezpieczeństwa, co raczej wygody, ułatwień codziennego funkcjonowania w przestrzeni publicznej. Zdaje się, że niepomni na lekcje dziejów łatwo i bez większych oporów oddajemy swą wolność, a nierzadko i godność. Jakże proroczo brzmią i dziś słowa Étienne de La Boétie z 1576 roku: „Lud sam oddaje się w niewolę i podrzyna sobie gardło; mogąc wybrać poddaństwo albo swobodę, odrzuca wolność i przyodziewa jarzmo; przystaje na niedolę czy raczej jej szuka"[54]. Słabość reakcji na ujawniane informacje odnośnie do skali inwigilacji, jakiej jesteśmy

[51] Por. tamże, s. 14.
[52] Tamże, s. 24.
[53] Por. P. Szostak, *Ściemniaj, aż ci się uda*, „Gazeta Wyborcza" 16–17 listopada 2019, s. 18; Kai-Fu Lee, *Inteligencja sztuczna, rewolucja prawdziwa. Chiny, USA i przyszłość świata*, tłum. K. Hejwowski, Warszawa 2019.
[54] É. de La Boétie, *Rozprawa o dobrowolnej niewoli*, tłum. K. Matuszewski, Katowice 2008, s. 10.

poddawani, a przykład Roberta Snowdena jest najbardziej jaskrawy, świadczy, że jako społeczeństwa jesteśmy raczej pogodzeni z nadzorem i konsekwencjami z niego płynącymi.

EKSKURS II. ANTYNOMICZNOŚĆ WARTOŚCI A ICH KONFLIKT: W KRĘGU ROZRÓŻNIEŃ NICOLAIA HARTMANNA

Nicolai Hartmann, nawiązujący w XX-wiecznej etyce do Arystotelesa, Kanta i fenomenologii, wprowadził istotne rozróżnienie między antynomią dóbr-wartości a ich konfliktem[55]. W pierwszym wypadku chodzi o sytuację, w której dwie wartości pozytywne pozostają w radykalnej opozycji, ich połączenie jawi się jako niezwykle trudne lub wręcz niemożliwe („niewspółwykonalność zasadnicza"). Przykładem jest duma i pokora, sprawiedliwość i miłość, pełnia życia i czystość moralna, miłość bliźniego i miłość dalekiego, obcego etc.[56]. Antynomiczność ma źródło w samych wartościach, ich „idealnej treści", jak mówił Hartmann. Natomiast konflikty wartości wynikają z niemożliwości empirycznej zrealizowania dwóch pozytywnych wartości jednocześnie („niewspółwykonalność empiryczna"). Ich przezwyciężanie jest możliwe choćby na drodze syntezy wartości (*Wertsynthese*), czego najlepszym przykładem jest cnota u Arystotelesa. Generalnie antynomiczność jest dla Hartmanna teoretycznie nieprzezwyciężalna, a konflikty moralne stanowią sam rdzeń życia moralnego człowieka, który musi je podmiotowo rozwiązywać poprzez podjęcie określonej decyzji, kierując się indywidualną i niedyskutowalną intuicją moralną o charakterze emocjonalnym[57].

Warto tu też przywołać prawo mocy wartości Hartmanna, odróżniające moc (*Wertstärke*) oraz wysokość (*Werthöhe*) i orzekające, że wartości

---

[55] Por. N. Hartmann, *Ethik*, Berlin-Leipzig 1962, s. 294–335 oraz 534–620. W tym dziele Hartmann w sposób bardzo szeroki i posługując się przykładami, omawia tę kwestię. Syntetycznie pisze o niej w: *Wprowadzenie do filozofii. Autoryzowany zapis wykładu wygłoszonego w semestrze letnim 1949 roku w Getyndze*, tłum. A.J. Noras, Warszawa 2000, s. 178–180 i 201–208. Por. J. Galarowicz, *Fenomenologiczna etyka wartości*, t. 1, Kraków 1997, s. 201–206; Z. Zwoliński, *Byt i wartość u Nicolaia Hartmanna*, Warszawa 1974, s. 365–370; W. Galewicz, *N. Hartmann*, Warszawa 1987, s. 163–167.

[56] Por. N. Hartmann, *Wprowadzenie do filozofii*…, s. 178–180.

[57] Słusznie w kontekście myśli Hartmanna zauważa Włodzimierz Galewicz: „Właściwą drogą do wartości nie jest bowiem dialektyczna konstrukcja, lecz emocjonalna intuicja" (W. Galewicz, *N. Hartmann*…, s. 167).

wyższe domagają się preferencji ze względu na ich wysokość w hierarchii wartości, a niższe ze względu na ich moc, siłę, wynikającą z fundamentalności. Dla przykładu, wartości kulturowe są wysokie, ale słabe, a witalne niskie, ale silne. Wśród wartości *stricte* moralnych niższą – ale silniejszą – jest sprawiedliwość, a wyższą – ale słabszą – miłość. Wartości niższe w swej fundamentalności „dźwigają moralność", a dopiero wyższe nadają sens ludzkiemu życiu. Hartmann interpretuje cnoty u Arystotelesa jako połączenie dwóch wartości (pozytywne są przeciwstawne, a negatywne bez problemu się łączą). Im wyższą wartość realizujemy, tym mamy większą moralną zasługę, a im niższą, bardziej fundamentalną gwałcimy, tym większa nasza wina moralna. Nierzadko należy dawać pierwszeństwo wartościom niższym z powodu ich fundamentalności, stanowią przecież warunki wartości wyższych.

Niemiecki etyk ostrzega przed „tyranią wartości", czyli zafiksowaniem się na określonej wartości, uczynieniem jej tyranem swego etosu i absolutyzowaniem jej (co zazwyczaj kończy się jakąś formą fanatyzmu), gdyż każda jest jednostronna i niepełna. Fundamentem, dzięki któremu człowiek jest odniesiony do wartości i staje się podmiotem odpowiedzialnym, jest wolność. „Wolność jest trzecim orzecznikiem boskości, do którego człowiek musi sobie rościć pretensję, jeśli rzeczywiście chce istnieć jako istota odpowiedzialna i moralna"[58]. Zauważmy w tym kontekście, że wolność jawi się jako metawartość o najbardziej fundamentalnym charakterze dla egzystencji człowieka, warunkiem bycia istotą moralną[59], a z drugiej jest to wartość wysoka. Zatem jej charakter fundamentu życia osobowego człowieka nadaje jej szczególną rangę i znaczenie jako wartości konstytuującej osobę[60]. Przejdźmy zatem do pytania o prymat tytułowych dóbr osoby ludzkiej.

PYTANIE O PRYMAT

Wolność człowieka jest w klasycznej wizji antropologicznej fundamentem struktur osobowych, posiada zatem charakter dobra dla człowieka pierwotnego wobec wszystkich jakościowych uposażeń. Przy czym nigdy nie jest ona absolutna, zawsze posiada wielorakie ograniczenia, wynika-

[58] N. Hartmann, *Wprowadzenie do filozofii*…, s. 137.

[59] Słusznie pisał Józef Tischner: „wolność jest środkiem nieodzownym do tego, by człowiek mógł tworzyć siebie jako istotę moralną" (J. Tischner, *Świat ludzkiej nadziei*, Kraków 1975, s. 66).

[60] Por. N. Hartmann, *Ethik*…, s. 345–351.

jące ze wspólnotowego bytowania człowieka. Wolność określa sferę indywidualności człowieka, dobrze wpisując się w boecjańską definicję osoby ludzkiej. Wartość bezpieczeństwa natomiast chroni byt człowieka w jego fizycznej i psychicznej integralności, wyzwala od lęku. Charakter aksjologiczny bezpieczeństwa jest zbliżony bardziej do potrzeb fizycznych, związanych z zachowaniem życia i zdrowia. Mając równie fundamentalny charakter, ustępuje w kwalifikacji osobowej wolności. W swych wyborach dokonywanych w sytuacjach konfliktowych ludzie mają różne preferencje. Erich Fromm opisał zjawisko ucieczki od wolności, wskazując na takie jej mechanizmy, jak: autorytaryzm, destruktywność i konformizm. Wolność wszak pociąga za sobą odpowiedzialność, a ta niesie za sobą zobowiązania, często trudne, nierzadko na granicy heroizmu. Ucieczka od wolności jest ucieczką od moralnej odpowiedzialności, zdaje się prowadzić do łatwego życia. Można w tym kontekście przytoczyć takie przykłady, jak biblijna wędrówka Żydów na pustyni, którzy stawiali bezpieczeństwo ponad wolność, czy wybory wielu Niemców w czasie II wojny światowej. Zjawisko to jest wyraźnie nacechowane negatywnie. Ucieczka od wolności to poniekąd ucieczka od siebie, od własnego człowieczeństwa, w jego rdzennej wartości. Z kolei przykłady cierpienia za wolność, a nawet oddawania życia w imię wolności, dla wolności, w walce o wolność, spotyka się z powszechną intuicyjną aprobatą i podziwem, co wyraźnie wskazuje, że wolność stanowi fundament osobowych struktur życia człowieka. Priorytet wolności wobec bezpieczeństwa jawi się nie tylko jako wniosek płynący z określonej antropologii filozoficznej, ale jest głęboko zakorzeniony w świadomości człowieka. Wolność wszak zakłada możliwość partycypowania w świecie wartości, dokonywania wyborów, podejmowania decyzji, choćby tych o wyborze wartości hedonicznych czy witalnych. Także Kościół, mówiąc o możliwości i prawie do ograniczania w pewnych sytuacjach ludzkiej indywidualnej wolności w imię dobra wspólnego, słowami konstytucji soborowej zastrzega: „z chwilą zmiany warunków należy natychmiast przywrócić swobodę" (KDK 75). Warto też podkreślić, że lęk przed wolnością nierzadko bierze się z poczucia braku bezpieczeństwa właśnie, poczucia samotności, co powoduje niechęć do decydowania o sobie, podejmowania określonych działań.

W jakich obszarach pojawia się w przypadku obu analizowanych dóbr-wartości wykluczanie, napięcie, a w jakich symbioza, współwarunkowanie? Różne zachodzą relacje między obu wartościami: warunkowanie (wolność od zagrożeń jako forma bezpieczeństwa), dopełnianie (cnoty jednostkowe – wolność a cnoty społeczne, wspólnotowe – bezpieczeństwo) lub wykluczanie (wybór bezpieczeństwa

kosztem wolności lub społeczne narzucanie ograniczeń wolności poprzez różne formy inwigilacji). Czy zachodzi między nimi – przynajmniej czasem – hartmannowska antynomiczność czy konfliktowość wartości? Wydaje się, że nie ma między nimi antynomiczności. Wręcz przeciwnie, w swej „idealnej treści" zdają się one wzajemnie warunkować. Natomiast sytuacje faktycznego życia społecznego, ze szczególnym uwzględnieniem wzrastających przestrzeni inwigilacji, prowadzą do konfliktowania obu dóbr ludzkiego życia. Im więcej bezpieczeństwa, słyszymy, tym mniej wolności – trzeba wybierać, a w dobie rozlicznych radykalnych niebezpieczeństw wybór wydaje się prosty. Tym bardziej, że przywykliśmy do ograniczania wolności i kurczenia swej prywatności w dobie Internetu i niesionych przez niego wyzwań oraz wabików.

W inwigilacyjne zabiegi mające rzekomo zapewnić obywatelom wzrost bezpieczeństwa jest wpisana głęboka ambiwalencja. Z jednej strony chcemy być bezpieczni, z drugiej, wiele środków prawdziwie czy fałszywie temu sprzyjających odbieramy jako naruszenie nie tylko struktur naszej prywatności i wolności, ale i samego bezpieczeństwa. Symbolem nieustannej inwigilacji jest „oko Boga", które wszystko percypuje, nad wszystkim w jakiś fundamentalny sposób czuwa, wszystkiego „dogląda". I tu mamy ambiwalencję. Z jednej strony jawi się idea Opatrzności, która troskliwie czuwa nad naszymi losami, jest wyrazem zatroskania o nasz byt, a z drugiej strony świadectwo Jeana-Paula Sartre'a, którego idea „oka Boga" doprowadziła do dziecięcego ateizmu. Skoro Bóg wszystko widzi, to moja wolność jest pozorem, a prywatność nie istnieje. Trzeba też pamiętać o ważnym sprzężeniu zwrotnym: im więcej technicznych zabezpieczeń, tym bardziej wzrasta poczucie nie-bezpieczeństwa, zagrożenia, rodzi się swoista obsesja bezpieczeństwa, która z pełnym zrozumieniem podchodzi do kurczenia się sfery wolności i prywatności ludzi. A nowe wynalazki cyberprzestrzeni tylko na to czekają, oferując coraz to nowsze sposoby inwigilacji, stwarzając oczywiście pozory, że śledzenie równa się czuwaniu. Zarządzanie lękiem, poczuciem zagrożenia, to jeden z ważnych sektorów rządzenia i manipulowania.

Obie wartości, zarówno wolność i skorelowana z nią sfera prywatności, indywidualności, oraz bezpieczeństwo we wszystkich swych aspektach są dla człowieka ważne, choć stan twórczej równowagi między nimi staje się trudno osiągalny[61]. Wzrost wolności prowadzi

[61] „Godne i satysfakcjonujące ludzkie życie jest nie do pomyślenia bez domieszki zarówno wolności, jak i bezpieczeństwa, w praktyce jednak rzadko udaje się osiągnąć szczęśliwą równowagę między tymi dwoma wartościami" (Z. Bauman, *Płynne życie*, tłum. T. Kunz, Kraków 2007, s. 59).

często do poczucia zmniejszenia bezpieczeństwa i na odwrót. Rzadko jednak mamy do czynienia z radykalnym przeciwstawieniem obu wartości. Niebezpieczeństwo czasów współczesnych z ich technikami prawdziwie lub pozornie zabezpieczającymi wolność lub dającymi – choćby w przestrzeniach konsumpcjonizmu – złudne poczucie wolności, polega na powolnym oswajaniu nas ze zmniejszaniem sfery wolności z jednej strony, a z drugiej na naszej mniej lub bardziej świadomej zgodzie na taki stan rzeczy. Konfliktowość w ten sposób przybiera postać mało znaczącego dla życia problemu. Gdyby jednak nasze tytułowe pytanie oczekiwało jednoznacznej odpowiedzi, to należałoby wskazać na wyraźny prymat wolności nad bezpieczeństwem ze względu na specyfikujący osobę ludzką charakter tej pierwszej wartości.

ZAKOŃCZENIE

Podsumowując, należy zauważyć, że bezpieczeństwo w aspekcie klasycznej koncepcji człowieka jest dobrem niższym, ale bardziej fundamentalnym w aspekcie istnienia człowieka jako bytu, natomiast wolność rysuje się jako fundament wszelkich jego struktur osobowych, trzeba ją zatem uznać za wartość wyższą. Niemniej mamy do czynienia z dwiema wartościami fundamentalnymi, warunkującymi wręcz ludzką egzystencję. Wolność możemy uznać za metawartość, stanowiącą *conditio sine qua non* wszelkich odniesień człowieka do świata dobra i wartości, w tym warunek przyjęcia wolności faktycznej tudzież jej odrzucenia („ucieczka od wolności"). Zrost wolności z człowieczeństwem podkreślają wszystkie właściwie klasyczne wizje człowieka, a Jan Jakub Rousseau wyraźnie do nich nawiązał, pisząc: „zrzec się swej wolności, to zrzec się swego człowieczeństwa"[62]. Podobnie Hegel, wskazując na to, że wolność jest istotą ducha[63]. Jean-Hervé Lorenzi i Mickaël Berrebi w odniesieniu do teraźniejszości zauważają:

„Wydaje się, że prywatność jest tym obszarem, który w tej chwili ma dla nas największe znaczenie, i to w skali globalnej. Wszyscy doskonale widzimy, że jesteśmy śledzeni, stale nadzorowani i poddawani wpływom firm, które przy okazji świadczenia usług, określają nasze profile i wykorzystują je do optymalizacji swoich kampanii marketingowych

[62] J.J. Rousseau, *Umowa społeczna, czyli zasady prawa politycznego*, tłum. A. Peretiatkowicz, Łódź 1948, s. 15.
[63] Por. G.W.F. Hegel, *Wykłady z filozofii dziejów*, t. 1, tłum. J. Grabowski, A. Landman, Warszawa 1958, s. 26.

i systemów sprzedaży. To jednak dopiero początek, który w dodatku nie stanowi niespodzianki, ponieważ wszystko odbywa się za naszą zgodą. Geolokalizacja nie jest już okazjonalna, ale stała. Jednak przerażającą granicę przekroczono w dziedzinie kontroli naszej własnej woli. Znajomość danego człowieka jest i będzie tak duża, że ostatecznie będzie miała wpływ na jego zachowanie. W tym przypadku bez wahania można mówić o mechanizmie samospełniającego się proroctwa, to znaczy o niemal trwałej utracie naszej wolności wyboru jako jednostek"[64].

Warto zwrócić uwagę na dość radykalną ambiwalencję we współczesnym rozumieniu wolności. Z jednej strony mamy jej bezwzględną liberalną akceptację, z drugiej negację wolnego ośrodka decyzji w człowieku poprzez wskazywanie na wszelkie determinizmy biologiczno-genetyczne, psychologiczne, środowiskowe, wychowawcze etc. Zresztą czasy, w których żyjemy, raczej nie cenią koherencji jako wartości epistemicznej.

Pamiętając o możliwości tyranii wartości, trzeba z jednej strony wystrzegać się absolutyzacji bezpieczeństwa, która z istoty jest względna i cząstkowa, ale i absolutyzacji wolności (która wszak też jest zawsze ograniczona) oraz autonomii, choćby w duchu Sartre'a, który zresztą z jednej strony definiował człowieka poprzez „świadomość wolności", z drugiej natychmiast podkreślał tragizm ludzkiego bytowania, w którym jesteśmy „skazani na wolność", wolność staje się dla nas przekleństwem. Optymalną drogą zdaje się zdążanie ku równowadze obu dóbr, co być może jest wyrazem naiwnego optymizmu. Bezpieczeństwo strzeże pewnego typu ładu, istniejących wartości, których wystarczy nie naruszać. Podobnie prywatność. Wolność realizuje się w aktach osobowych człowieka, jest wartością domagającą się realizacji. Wolność odpowiedzialna bierze pod uwagę wymogi społecznego dobra wspólnego, wymogi prawidłowego funkcjonowania państwa, jego organizacji, struktur etc. w wypełnianiu właściwych mu funkcji i zadań. Prywatność w jakiejś mierze musi ustępować wymogom płynącym z ochrony istniejącego ładu społecznego, z kolei bezpieczeństwo i jego imperatywy nie mogą istotnie ograniczać wolności jednostek, szczególnie wolności egzystencjalnej, wyrażającej się w określonym „poczynaniu samego siebie", wolności wyrażającej się w „działaniu ze zrozumienia", a nie posłuszeństwa czy samowoli (Jaspers). Poczucie bezpieczeństwa jest wszak jakimś warunkiem pełnego cieszenia się wolnością, a nie jej antynomicznym znoszeniem. Obie wartości są niezwykle ważne

[64] J.-H. Lorenzi, M. Berrebi, *Przyszłość naszej wolności*..., s. 226.

dla egzystencji człowieka, a sytuacje ich konfliktu czy świadomego rozgrywania ich przeciw sobie należy uznać za deformację aksjosfery człowieka.

Wolność jest wezwaniem do samodzielności, do bycia sobą, do realizacji własnego planu życia, jest warunkiem autentyczności bytowania. Fundamentalny wybór wolności lub jej odrzucenia w różnych postaciach ucieczki pociąga za sobą wybór siebie jako osoby lub ucieczkę od siebie. Taka lekcja płynie z klasycznej antropologii filozoficznej. Gra toczy się zatem o wielką stawkę, o moje/nasze człowieczeństwo. Jego sens i istotę w gąszczu rozmaitych propozycji aksjologicznych łatwo przegapić. Zdaje się, że coraz łatwiej…

CZY PLOTKA PRZETRWA REWOLUCJĘ INFORMATYCZNĄ? LOS NIEFORMALNYCH MECHANIZMÓW KONTROLI SPOŁECZNEJ W CYBERŚWIECIE

RADOSŁAW SOJAK

Instytut Socjologii UMK

W dobie plotkarskich portali, tabloidowej prasy i wszędobylskich *paparazzi* stawianie tytułowego pytania może wydawać się aż nadto prowokacyjne. Nie o samą prowokację i pobudzenie uwagi Czytelników jednak chodzi, tak samo jak nie chodzi nam o samą plotkę. Ta ostatnia występuje tu bowiem przede wszystkim jako figura, retoryczne zastępstwo i egzemplifikacja tego, co socjologowie nazywają nieformalnymi mechanizmami kontroli społecznej[1]. Istota naszego pytania sprowadza się więc do tego**, jak w dobie rewolucji cyfrowej funkcjonować będą nieformalne mechanizmy kontroli społecznej?**

Odpowiedzi na tak przeformułowane, tytułowe pytanie postaramy się udzielić w kilku zdyscyplinowanych krokach: (1) najpierw wyartykułujemy kilka nieoczywistych założeń leżących u podstaw przedstawionego tu rozumowania, (2) następnie poświęcimy nieco uwagi naturze i sposobowi działania nieformalnych mechanizmów kontroli społecznej, (3) potem pochylimy się nad kilkoma standardowymi ścieżkami myślenia o konsekwencjach rewolucji cyfrowej, (4) zaproponujemy własną hipotezę dotyczącą możliwych konsekwencji cyfrowej rewolucji.

[1] Zob. np.: A.B. Hollingshead,*The Concept of Social Control*, American Sociological Review 6, nr 2/1941, ss. 217–224.

ZAŁOŻENIA

Plastyczność i różnorodność kultur oraz sposobów organizacji społeczeństw ludzkich stanowiła dla nauk społecznych przez dekady ważki problem badawczy, dostarczała wielu ciekawych przedmiotów badań, stanowiła nawet podłoże dla powstania odrębnych, w pełni samodzielnych dyscyplin naukowych (np. antropologii kulturowej). Jednocześnie jednak fascynacja ową różnorodnością utrudniała dostrzeżenie, iż swoista „gra w społeczeństwo" odbywa się nie tylko na podłożu biologicznym (jak chciał chociażby Alfred Kroeber w swojej koncepcji ewolucji ponadorganicznej[2]), ale raczej w ramach dość ściśle określonych warunków brzegowych wyznaczanych ewolucyjną historią gatunku *homo sapiens sapiens*. I to właśnie stanowi podstawowe założenie poniższej analizy: **niezależnie od plastyczności urządzeń społecznych są one zawsze rodzajem adaptacji do biologicznych właściwości człowieka**. Takie elementy jak średnia długość życia, następstwo pokoleń, dualizm płciowy, poziom naszych zdolności poznawczych, wzrokowy charakter doświadczania świata, objętość pamięci średnio- i długookresowej to swoiste stałe biologiczne. Ulegają one wprawdzie modyfikacjom pod wpływem kultury, ale większość tych modyfikacji nie zdołała się jeszcze zakorzenić w naszym uposażeniu biologicznym. By użyć stosownej dla tematyki tego tomu metafory – większość tych modyfikacji to nadal *software*, a nie *hardware* naszego gatunku. Nawet jeśli założymy, że człowiek w kulturze żyje ok. 15 tys. lat (a założenie to dość optymistyczne), to jest to okres zdecydowanie zbyt krótki, by nasze przystosowanie do kultury mogło zakorzenić się genetycznie (podążam tu za dobrze znaną argumentacją Edwarda O. Wilsona i całej tradycji socjobiologicznej[3]).

Przyjęcie powyższego założenia sprawia, że w odniesieniu do rzeczywistości społecznej musimy zaakceptować perspektywę umiarkowanego konstruktywizmu – w duchu chociażby Niklasa Luhmanna[4] czy Harrisona C. White'a[5]. Stanowisko takie zakłada, że **wszelkie instytucje społeczne mają charakter adaptacyjny i są względnie trwałymi kon-**

---

[2] A.L.Kroeber, *Istota kultury*, Warszawa, PWN, 1973.

[3] E.O. Wilson, *Sociobiology. The Abridged Edition*; *Sociobiology: The New Synthesis*, Harvard University Press, 1975.

[4] N. Luhmann, *Systemy społeczne. Zarys ogólnej teorii*, Kraków, Zakład Wydawniczy Nomos, 2007.

[5] H.C. White, *Identity and Control: How Social Formations Emerge* (Second Edition), Princeton, NJ, Princeton University Press, 2008.

strukcjami o przynajmniej częściowo arbitralnym charakterze. Taki umiarkowany konstruktywizm od stanowisk bardziej radykalnych odróżnia przede wszystkim założenie najpełniej wyartykułowane w stwierdzeniu Luhmanna: „żaden konstruktywista […] nie zaprzeczy, że konstrukty muszą powstawać na drodze realnych, czułych na środowisko operacji"[6]. Innymi słowy, stwierdzenie, że coś jest konstrukcją społeczną, nie jest równoważne stwierdzeniu, iż owo „coś" może być w zasadzie dowolne. Konstruowanie to zawsze proces negocjacji, uzgadniania koniecznych ustępstw i warunków brzegowych, których nie da się zignorować. Kształt instytucji społecznych jest więc pochodną wielu czynników, wśród których elementy wewnątrzspołeczne (np. dostępne technologie) są równie istotne jak czynniki środowiskowe czy biologiczne.

Wśród tych różnych warunków brzegowych ograniczających społeczną plastyczność naszych instytucji jedno z kluczowych miejsc zajmuje przemoc. To właśnie trzecie założenie poniższej analizy. Nie będzie przesadą, gdy za Peterem L. Bergerem powtórzymy, że „przemoc jest ostateczną podstawą każdego porządku politycznego"[7]. Ważne jednak, by tego stwierdzenia nie rozumieć jednowymiarowo. Porządek społeczny – każdy – jest do pewnego stopnia efektem zastosowania jakichś form przemocy. Jednocześnie jednak powstaje on zawsze po to, by owo użycie przemocy regulować, a najczęściej – ograniczać. W tym sensie przemoc jest zawsze podskórną groźbą każdego porządku społecznego, ale jej obecność ma być możliwie zawoalowana. Dotyczy to w szczególności nowoczesnych społeczeństw wysoko rozwiniętych, o których można wręcz powiedzieć, że popadają w skrajność utopijnego przekonania, że istnieje możliwość zbudowania porządku społecznego całkowicie pozbawionego przemocy (tak np. można rozumieć skrajne przejawy poprawności politycznej czy tzw. *wokeculture*). Ta wyjątkowa rola przemocy wynika zapewne z faktu, iż jest ona swoistym uniwersalnym językiem komunikacji. Gdy zawiodą wszystkie inne sposoby, pozostaje tylko przemoc – skuteczna niezależnie od wszystkich możliwych różnic biologicznych, społecznych, kulturowych. Gra w społeczeństwo toczy się zaś o to, byśmy mieli do dyspozycji możliwie bogaty wachlarz „wszystkich innych sposobów", nim trzeba będzie uciec się do przemocy.

---

[6] N. Luhmann,*Observations on Modernity*, Stanford, CA: Stanford University Press, 1998, s. 12.

[7] P.L. Berger, *Zaproszenie do socjologii*, Warszawa, Wydawnictwo Naukowe PWN, 1988.

NIEFORMALNA KONTROLA SPOŁECZNA

Jest wiele przenikliwości w przypisywanej Ervingowi Goffmanowi definicji człowieka jako „zwierzęcia unikającego gaf" (*gaffe-avoidinganimal*)[8]. Błyskotliwość tego konceptu często jednak sprawia, że jego analityczna głębia nie jest w pełni doceniana. Cóż bowiem oznacza nasza predylekcja do unikania gaf? Czy tylko strach przed śmiesznością? Czy tylko chęć bycia *commeilfaut* w towarzystwie? Zdecydowanie nie.

Na najgłębszym poziomie skłonność do unikania gaf oznacza chęć bycia przewidywalnym, zachowania się zgodnie z oczekiwaniami innych uczestników interakcji. I właśnie złożone systemy kontroli społecznej funkcjonujące we wszystkich znanych nam społeczeństwach służą osiąganiu tego celu. Możemy go nazywać konformizmem, możemy – koordynacją działań zbiorowych, możemy – uwewnętrznieniem norm społecznych. Niezależnie od nomenklatury sens i cel będą takie same: tak zorganizować życie społeczne, by zapewnić przewidywalność, a zatem bezpieczeństwo interakcji między ludźmi. Wchodząc do pociągu, na salę wykładową czy do gabinetu lekarskiego, oczekujemy, że często zupełnie obcy ludzie, których tam spotkamy, będą zachowywali się w pewnych granicach standardowo – przewidywalnie, mimo że co do zasady wiemy, jak bardzo zaskakujące i idiosynkratyczne potrafią być zachowania przedstawicieli naszego gatunku.

To właśnie systemy kontroli społecznej oparte na początkowej inkulturacji, a później instytucjonalnym egzekwowaniu norm zapewniają nam ową przewidywalność, czy też w nomenklaturze Anthony Giddensa – „bezpieczeństwo ontologiczne"[9]. Problem w tym, że myśląc o nich z dzisiejszej, nowoczesnej perspektywy, nader często koncentrujemy się na tych ich aspektach, które mają sformalizowany charakter. Sformalizowany, tzn. oparty na prawie, czy szerzej – regułach pisanych, i egzekwowany instytucjonalnie. Z tej perspektywy w systemach kontroli społecznej widać w pierwszej kolejności system edukacyjny, sądy, policję, system penitencjarny. Tymczasem nadal zdecydowanie więcej naszych zachowań regulowanych jest bezpośrednio przez normy nieformalne – zwyczajowe, oparte na tradycji i obyczaju. To niezliczone normy i powinności, które formalny system prawny zamyka w eleganckiej formule „zasad współżycia społecznego". Zasad, które mają charakter pierwotny i… najprawdopodobniej ewolucyjny.

---

[8] Zob. np. E. Goffman, *Człowiek w teatrze życia codziennego*, Warszawa, PIW, 1977.

[9] A. Giddens, *Modernity and Self-Identity. Self and Society in the Late Modern Age*, Cambridge: Polity, 1991.

Rozpoznawanie twarzy innych ludzi to dość banalna z perspektywy większości jednostek codzienna czynność, której komputerowa emulacja okazała się niesłychanie skomplikowana. Dużo szybciej nauczyliśmy komputery rozpoznawać wzory linii papilarnych, tęczówek, a nawet odczytywać i „rozumieć" mowę, niż dokonać prawidłowej identyfikacji na podstawie wyglądu twarzy. Dlaczego tak złożona informacyjnie czynność został przez nasz gatunek tak doskonale wytrenowana? Jedna z hipotez sformułowanych przez psychologię ewolucyjną zakłada, że stało się tak właśnie po to, by mogły zaistnieć mechanizmy kontroli społecznej.

Rozumowanie, które rekonstruuję w tym miejscu za Robinem Dunbarem[10], przebiega w tym względzie mniej więcej tak. Człowiek jest zwierzęciem stadnym, którego ewolucja dokonywała się w sytuacji względnie stałego niedoboru żywności, a zatem deficytu energetycznego. W takich okolicznościach zdolność do przetrwania jednostek zależy od ich umiejętności współdziałania, koordynacji wysiłków oraz gotowości do dzielenia się zdobytymi zasobami. Innymi słowy, chodzi o to, by grupę tworzyły jednostki nastawione względnie altruistycznie wobec pozostałych członków. Rzecz w tym, że postawa altruistyczna wiąże się z koniecznością odkładania gratyfikacji w czasie. Z tej perspektywy szczególnie niebezpieczne staje się pojawianie się w grupie jednostek egoistycznych, które próbują „załapywać się" na zasoby zdobywane przez innych (teorie racjonalnego wyboru określają takie jednostki jako „jeźdźców na gapę"). Samo ich istnienie nie jest problemem – dobrze funkcjonująca grupa jest w stanie utrzymać zapewne ok. 5-10% egoistów. Kłopotem jest wszakże to, że ich obecność demoralizuje pozostałych – obniża skłonność do odsuwania gratyfikacji przez innych członków grupy, a w konsekwencji prowadzi do tego, że coraz więcej altruistów zamienia się w egoistów. Aby można było temu procesowi zapobiegać, trzeba egoistów stygmatyzować, a by ich stygmatyzować, trzeba ich rozpoznać – w warunkach naturalnych, bez imion, dowodów osobistych i PESEL-i. Tak właśnie mogła narodzić się paląca potrzeba skutecznego, szybkiego i trwałego rozpoznawania twarzy. I tak zapewne narodziła się interesująca nas plotka – podstawa większości znanych nam nieformalnych mechanizmów kontroli społecznej.

Plotka i plotkowanie nie mają dobrej prasy. Dobrowolna i powodowana ciekawością skłonność do dzielenia się (najczęściej niesprawdzo-

[10] R. Dunbar, *Grooming, Gossip and the Evolution of Language*, Harvard University Press, 1997; zob. także: L. Barrett, R. Dunbar, J. Lycett,*Human Evolutionary Psychology*, London: Palgrave, 2002.

nymi) informacjami na temat bliźnich nie uchodzi za cnotę. Skłonność do plotkowania różne kultury umieszczają jako istotny składnik niezbyt pochlebnych stereotypów. Niech nas jednak ten oficjalny obraz nie zmyli. Popularność plotkarskiej prasy czy portali internetowych oraz skłonność celebrytów do dzielenia się rozmaitymi szczegółami swojego prywatnego życia nie pozostawiają złudzeń. Plotka ma się dobrze – staje się swoistą *guiltypleasure* współczesnej kultury. Czy chodzi tu jedynie o mechanizm dobrze opisany w aforyzmie François de La Rochefoucauld: „Hipokryzja to hołd składany cnocie przez występek"; czy może mechanizm ów ma nieco głębszy sens?

I znów warto w tym kontekście uruchomić perspektywę ewolucyjną. Jeśli plotka w istocie była narzędziem identyfikowania i stygmatyzowania egoistów w grupach pierwotnych, to gra toczyła się o naprawdę wysoką stawkę. Możliwa tu sankcja wyrzucenia poza nawias wspólnoty oznaczała właściwie wyrok śmierci. Plotkowanie nie mogło być więc czynnością „bezkosztową", nieobarczoną ryzykiem. W związku z tym w większości kultur plotkowanie obrastało w liczne reguły ograniczające samą czynność oraz weryfikacji przekazywanych informacji. Niezależnie od tych reguł mechanizm pozostawał jednak ten sam i polegał na przypisywaniu jednostkom charakterystyk wpływających na ich pozycję społeczną we wspólnocie. I pod tym względem w epoce cyfrowej niewiele się zmienia. Nie znaczy to jednak, że nie zmienia się nic.

MEANDRY CYFROWEJ REWOLUCJI

Literatura dotycząca obecnych i spodziewanych konsekwencji rewolucji informatycznej jest olbrzymia, a sam obszar badawczy zaczyna powoli wybijać się na dyscyplinarną niezależność. Daje się tu jednak wyróżnić kilka powtarzających się wątków czy też paradygmatów[11]. Warto o najistotniejszych z nich wspomnieć, bo na ich tle łatwiej będzie naszkicować specyfikę proponowanego tu podejścia.

Pierwszy z nich można określić za Jeremy'm Rifkinem[12] paradygmatem końca pracy. Wiąże się on z dostrzeganiem i coraz bardziej za-

[11] Dobre streszczenie większości z nich przynosi praca: Andrzej Zybertowicz, Maciej Gurtowski, Katarzyna Tamborska, Mateusz Trawiński, Jan Waszewski, *Samobójstwo Oświecenia? Jak neuronauka i nowe technologie pustoszą ludzki świat*, Kraków, Wydawnictwo Kasper, 2015.

[12] J. Rifkin, *Koniec pracy. Schyłek siły roboczej na świecie i początek ery postrynkowej*, Wrocław,Wydawnictwo Dolnośląskie, 2001.

awansowanymi analizami zjawiska bezrobocia technologicznego. W największym skrócie chodzi o to, że postępująca informatyzacja kolejnych branż systematycznie zmniejsza zapotrzebowanie na ludzką pracę. Proces ten gwałtownie przyspieszył w latach dziewięćdziesiątych XX w., gdy komputery stały się na tyle wydajne i tanie, by rozpoczął się proces stopniowej informatyzacji usług. Argumentacja Rifkina odwołuje się do szerszej perspektywy historycznej, wskazując, że kolejne fale automatyzacji pracy dotykały najpierw rolnictwo, następnie przemysł, aż wreszcie – dzięki komputerom właśnie – usługi. Problem w tym, że po raz pierwszy nie widać, dokąd miałaby migrować zbędna w usługach siła robocza. W tym właśnie kontekście należy rozpatrywać powracające coraz częściej dyskusje dotyczące zasadności wprowadzenia „gwarantowanego dochodu minimalnego" dla wszystkich obywateli, niezależnie od ich statusu zawodowego.

Drugi wyraźnie wyodrębniony sposób myślenia o rewolucji informatycznej można określić paradygmatem końca prywatności. Zwraca się tu uwagę na wzrastające możliwości technologicznego nadzoru. Owe możliwości mają dwa wymiary. Pierwszy to pojawiające się techniki nadzoru „doskonałego" na poziomie jednostkowym, drugi to możliwość identyfikacji wzorów zachowań na poziomie całych populacji. Te ostatnie dzięki mediom społecznościowym i – przynajmniej częściowo – dobrowolnemu dostarczaniu przez nas samych olbrzymiej ilości danych na temat naszych aktywności w ostatnich latach weszły na zupełnie nowy poziom. Warto jednocześnie pamiętać, że niezależnie od tego, jak bardzo obezwładniające mogą nam się wydawać techniki nowoczesnego nadzoru, są one cały czas dalekie od uzyskania pełnego potencjału. Barierą pozostaje problem przetwarzania dużych baz danych. Problem, którego rozwiązaniu poświęca się wiele uwagi w ramach studiów z zakresu uczenia maszynowego, sztucznej inteligencji, architektury informacji i tzw. *big data*.

Warto wszakże w trybie komentarza socjologicznego zwrócić w tym miejscu uwagę, że prywatność, z którą być może przychodzi nam się właśnie powoli żegnać, była wynalazkiem nowoczesności. Trudno było o nią w nieprawdopodobnie zatłoczonych miastach starożytności i średniowiecza, tak samo jak w pełnych służby rezydencjach bogaczy różnych epok. Prywatność miała zupełnie inny smak, gdy domostwo było jednocześnie miejscem pracy, a dominujący model rodziny zakładał wspólną egzystencję minimum trzech pokoleń. Co więcej, w większości kultur pierwotnych, które zdążyliśmy poznać, chęć bycia w samotności uważana była z definicji za podejrzaną. Chęć izolacji od wspólnoty była podstawowym sygnałem nieczystych intencji. Może więc w tym akurat

względzie rewolucja informatyczna oznaczać będzie raczej powrót do „stanu naturalnego" niż pożegnanie z pozornie wrodzoną potrzebą człowieka.

Nie zmienia to faktu, że przedefiniowanie granicy między tym, co prywatne, i tym, co publiczne, wiąże się z trzecim, łatwym do wyodrębnienia, sposobem myślenia o konsekwencjach rewolucji informatycznej – nazwijmy go paradygmatem końca demokracji. Argumentacja w tym względzie czerpie z obu zrekonstruowanych dotąd sposobów myślenia. Przede wszystkim wskazuje, że dla powstania nowoczesnych demokracji kluczowe znaczenie miała koncentracja siły roboczej w wyniku procesu urbanizacji i uprzemysłowienia. Koncentracja, która z jednaj strony pozwoliła na koordynację działań dotąd rozproszonej siły roboczej, z drugiej zaś dała jej swoiste prawo weta. Demokracja powszechna w tym kontekście jawi się jako konieczny koszt utrzymania w ryzach warstw pracujących. W dobie globalnych przepływów i ogólnej redukcji znaczenia działalności produkcyjnej dla funkcjonowania gospodarek strajk paraliżujący strategiczne gałęzie przemysłu nie jest już jednak możliwy. Ale śmierć demokracji nie przychodzi jedynie dlatego, że przestaje się ona opłacać elitom. Drugi mechanizm, który się do tego przyczynia, to niespotykany dotąd wzrost możliwości manipulacji. Nasilające się zjawisko baniek informacyjnych, otaczania nas przez algorytmy stron internetowych i serwisów społecznościowych tylko tymi informacjami, które pasują do naszych wcześniejszych wyszukiwań i polubień, oznacza, że strukturalnie zanika podstawowy składnik demokracji – dobrze poinformowany obywatel[13]. Jeśli dodamy do tego wszechogarniające zjawisko szumu informacyjnego, to trudno się dziwić, że mechanizmy klasycznej oświeceniowej demokracji (nawet jeśli zawsze były jedynie wzniosłym postulatem) zdają się nieadekwatne w obliczu wyzwań współczesnego świata.

Czwarty wreszcie sposób myślenia o konsekwencjach rewolucji informatycznej bez większej przesady można określić mianem paradygmatu końca człowieczeństwa. Czasami chodzi tu o koniec w zupełnie dosłownym sensie, koniec spowodowany przejęciem kontroli nad światem przez zautonomizowany system sztucznej inteligencji, który najzwyczajniej może stwierdzić, że człowiek jest „zbędnym" elementem rzeczywistości. „Zbędnym", bo najmniej przewidywalnym, najbardziej skłonnym do popełniania błędów, najsłabszym… Czasami jednak w takich rozważaniach chodzi tylko o koniec człowieczeństwa takiego,

[13] Zob. np.: S. Wolin, *Democracy Incorporated: Managed Democracy and the Specter of Inverted Totalitarianism*, Princeton University Press, 2017.

jakie znamy. Tak jest na przykład wtedy, gdy transhumaniści snują wizje cyfryzacji ludzkiej świadomości i tym samym uwolnienia jej treści od śmiertelnego i niedoskonałego ciała.

W kontekście takich przewidywań rozważanie problemu przyszłości plotki – czy nawet szerzej – mechanizmów nieformalnej kontroli społecznej wydaje się mało doniosłe. Sądzę jednak, że może nas ono doprowadzić do niebanalnych wniosków.

BŁOGOSŁAWIONA NIEPAMIĘĆ

Plotka (i szerzej nieformalne mechanizmy kontroli społecznej) to ludzkie rozwiązania problemów ludzkich wspólnot. Rewolucja informatyczna jest dla nich groźna na dwa sposoby. Oba wiążą się z zagadnieniem pamięci.

W klasycznej komedii romantycznej *Notting Hill* jest scena dokładnie obrazująca dylemat funkcjonowania ludzkiej pamięci, o którym tu mowa. Bohaterka kreowana przez Julię Roberts, amerykańska gwiazda filmowa, przybiega roztrzęsiona, chowając się przed *paparazzi* do mieszkania niedawno poznanego, zwykłego, angielskiego pisarza (tylko przez przypadek granego przez Hugh Granta). Powodem roztrzęsienia jest odnalezienie i opublikowanie przez tabloidy roznegliżowanych zdjęć z początków kariery naszej bohaterki. W niezręcznym odruchu pocieszenia księgarz próbuje bagatelizować sprawę, zwracając uwagę, że przecież „dzisiejsze gazety wyścielą jutrzejsze kubły na śmieci". Mocno zdenerwowana tym argumentem bohaterka wykrzykuje w odpowiedzi, że od tej chwili każdy, kto będzie chciał cokolwiek o niej napisać, znajdzie bez problemu informacje o wstydliwych początkach jej kariery.

Ta scena jak w soczewce skupia dylematy związane z niemożnością naturalnego funkcjonowania nieformalnych narzędzi kontroli społecznej. To prawda, że są one oparte na możliwości rozpoznawania twarzy, polegają na naszej zdolności przypisywania innym ludziom charakterystyk i ich zapamiętywania. Jednocześnie jednak te zdolności pozostają ograniczone ułomnościami naszej pamięci. Jesteśmy w stanie utrzymywać tylko pewną skończoną liczbę trwałych i bezpośrednich relacji z innymi ludźmi, skutecznie rozpoznajemy twarze tylko ograniczonej liczby osób, pamiętamy wydarzenia tylko przez pewien czas. Innymi słowy, **w nieformalne mechanizmy kontroli wpisany jest nie tylko proces piętnowania, sądzenia i karania, ale także wybaczania i zapominania**. Wydaje się, że rewolucja informatyczna na dwa sposoby zaburza ten balans.

Hipoteza niechcianej trwałości. Geneza słynnej unijnej dyrektywy RODO wiąże się podobno z przypadkiem włoskiego przedsiębiorcy, który wiele lat po odbyciu kary i zatarciu prawnym wszelkich konsekwencji swoich zaległości podatkowych, nadal znajdował w przestrzeni internetowej informacje o bankructwie swojej firmy. Informacje, które negatywnie wpływały na jego możliwości prowadzenia biznesu. Nie sądzę, by unijna dyrektywa mogła zaradzić tego rodzaju problemom, właśnie dlatego, że dotyczą one mechanizmu dużo bardziej ogólnego. Mechanizmu niechcianej trwałości.

Wątek ten pojawia się powoli w kontekstach związanych z edukacją informatyczną dzieci i bezpieczeństwem w Internecie. Dorastają już kolejne pokolenia, które odkrywają, jak niezmiernie trudno jest z Internetu usunąć niezbyt przyzwoite zdjęcia, głupawe filmiki czy nadmiernie emocjonalne wpisy. W większości epok młodzi ludzie podejmowali różnego rodzaju nonkonformistyczne działania, często dość poważnie gwałcąc funkcjonujące normy swoich własnych wspólnot. Często bywali z tego powodu piętnowani. Ale jednocześnie owe wspólnoty najczęściej oferowały możliwość ekspiacji i dawały nadzieję na zapomnienie. Zapomnienie, które w związku z cyfrowym utrwaleniem staje się coraz trudniejsze. Nie musi tu zresztą chodzić o jakieś szczególnie drastyczne łamanie norm. Wystarczy zapytać, jak zmieniają się warunki dla psychologicznego procesu rozstania, gdy zdjęcia byłego partnera i jego nowej rodziny podsuwane są nam nieustannie przez bezduszne algorytmy Facebooka czy Instagrama?

Hipoteza nadmiernej precyzji. Trwa także w Polsce od jakiegoś czasu dyskusja na temat mowy nienawiści w Internecie. Podstawowy problem, jaki napotykają te dyskusje, wiąże się ze sformułowaniem prostej i łatwej w operacjonalizacji definicji „mowy nienawiści". Nie sądzę, by ten problem mógł zostać rozwiązany na gruncie prawnym. To, czy mowa przekracza dopuszczalne obyczajem granice agresji, podlegało zazwyczaj regulacjom nieformalnym, ocenie w pełnym kontekście danego aktu komunikacji i w sposób nieuchronnie arbitralny. Ta arbitralność, jakkolwiek kłopotliwa w kontekście sformalizowanych systemów prawnych, miała swoje zalety – pozwalała chociażby uwzględnić różne poziomy emocjonalnej wrażliwości osób uwikłanych w sporną komunikację. Cyfrowe utrwalenie komunikacji z jednej strony eliminuje znaczną część owego naturalnego kontekstu, który na czatach i forach nieudolnie próbujemy suplementować przy pomocy emotikonów, z drugiej jednak domaga się trudnej do osiągnięcia precyzji w kwestii oceny treści i intencji owej komunikacji.

Innymi słowy, **kontekst cyfrowy domaga się precyzji osądu, którego nie mogą zapewnić nieformalne mechanizmy kontroli, formalne zaś nie mogą sobie poradzić z naturalną indeksykalnością i wieloznacznością ludzkiej komunikacji**. Jak na razie jedyną odpowiedzią na ten dylemat, którą udało nam się odnaleźć, jest postępująca rozbudowa systemów prawnych regulacji.

Jaki więc los czeka w tym kontekście plotkę? Bez wątpienia nie zniknie ona z ludzkiego świata, ale grozi jej utrata ludzkiego wymiaru. Cyfrowo utrwalona i informatycznie precyzyjna utraci swój nieformalny, niezobowiązujący i poczciwy charakter. Okaże się, że będzie skazywać na towarzyską, społeczną, a nawet fizyczną banicję z precyzją i nieuchronnością, o której wyroki sądów mogłyby tylko pomarzyć…

NOTY O AUTORACH

DR INŻ. MICHAŁ SZYCHOWIAK
pracuje w Instytucie Informatyki Politechniki Poznańskiej od 1994 roku. Jest naukowcem, wykładowcą współpracującym z wieloma uczelniami, członkiem rad programowych konferencji naukowych i przemysłowych poświęconych systemom rozproszonym, bezpieczeństwu i niezawodności. Jego zainteresowania naukowe dotyczą dziedziny wiarygodności przetwarzania danych, w tym w szczególności dwóch obszarów – bezpieczeństwa systemów informatycznych oraz mechanizmów wysokiej niezawodności. Jest również organizatorem corocznych zawodów PUT Cybersecurity Capture the Flag, w których z praktycznymi problemami bezpieczeństwa cybernetycznego mierzą się studenci kierunków informatycznych i przedstawiciele przemysłu z kraju i z zagranicy.

DR INŻ. MACIEJ MIŁOSTAN
jest związany z Politechniką Poznańską, w której uzyskał tytuł doktora nauk technicznych w dyscyplinie informatyki w 2007 roku. Jego zainteresowania badawcze oscylują wokół zastosowania metod badań operacyjnych, uczenia maszynowego i przetwarzania danych na polu bezpieczeństwa teleinformatycznego oraz w zastosowaniach bioinformatycznych. Aktualnie jego podstawowym miejscem zatrudnienia pozostaje Politechnika Poznańska (od 2000 roku), ale współpracuje on również z Poznańskim Centrum Superkomputerowo-Sieciowym (od 2003 roku). Ma szerokie doświadczenie praktyczne w dziedzinie bezpieczeństwa uzyskane w wyniku wieloletniej administracji systemami IT, pracy związanej

z obsługą incydentów, udziałem w audytach bezpieczeństwa oraz projektach badawczo-rozwojowych finansowanych ze źródeł krajowych i europejskich. Ponadto prowadzi zajęcia dydaktyczne z ochrony danych i kryptografii. Jest współautorem szeregu publikacji zarówno z zakresu bezpieczeństwa teleinformatycznego, jak i bioinformatyki.

PROF. DR HAB. KRZYSZTOF STACHEWICZ,
filozof, teolog, historyk. Kierownik Zakładu Filozofii i Dialogu na Wydziale Teologicznym UAM w Poznaniu, redaktor naczelny rocznika naukowego „Filozofia Chrześcijańska". Autor wielu książek, artykułów i rozpraw. Ostatnio wydał: *Milczenie wobec dobra i zła. W stronę etyki sygetycznej i apofatycznej* (2013) oraz *Doświadczyć prawdziwej rzeczywistości. Prolegomena do filozofii mistyki* (2019). Główne przestrzenie badawcze: etyka, metaetyka, filozofia zła, antropologia filozoficzna, filozofia mistyki.

DR HAB. RADOSŁAW SOJAK, PROF. UMK
kierownik Zakładu Socjologii Ogólnej i Historii Socjologii.

– Zainteresowania badawcze:
socjologia wiedzy, teoria socjologiczna, analiza dyskursu, tajność jako kategoria socjologiczna, zakulisowe wymiary życia społecznego.

– Przebieg kariery:
- w roku akademickim 1997/98: asystent stażysta w Instytucie Socjologii UMK;
- w czerwcu 1998: egzamin magisterski na podstawie pracy pt. *Porządki wykluczeń. Ekskluzja społeczna w świetle socjologii wiedzy na przykładzie dyskusji wokół lustracji* – ocena na dyplomie bardzo dobra;
- od października 1998: asystent w Zakładzie Socjologii Ogólnej i Historii Socjologii Instytutu Socjologii UMK;
- w czerwcu 2002: zamknięcie przewodu doktorskiego na podstawie rozprawy pt. *Socjologia wiedzy w poszukiwaniu perspektywy ogólnej teorii społeczeństwa* napisanej pod kierunkiem dra hab. Andrzeja Zybertowicza, prof. UMK;
- od sierpnia 2002: adiunkt w Zakładzie Socjologii Ogólnej i Historii Socjologii Instytutu Socjologii UMK;

- od stycznia 2004: adiunkt w Zakładzie Interesów Grupowych Instytutu Socjologii UMK;
- od 2004 do 2007: zastępca dyrektora Instytutu Socjologii UMK ds. dydaktycznych;
- od 2007 do 2016: prodziekan Wydziału Humanistycznego UMK;
- od 2015 roku kierownik Zakładu Socjologii Ogólnej i Historii Socjologii,

– poza tym:

- od 1997 roku członek Polskiego Towarzystwa Socjologicznego;
- stypendysta Fulbrighta (1998), Fundacji na rzecz Nauki Polskiej (2000) oraz tygodnika „Polityka" w ramach akcji „Zostańcie z Nami!" (2006);
- autor rozprawy *Paradoks antropologiczny. Socjologia wiedzy jako perspektywa ogólnej teorii społeczeństwa* (Wrocław 2004) oraz współautor pracy *Zagubiona rzeczywistość. O społecznym konstruowaniu niewiedzy* (Warszawa 2005 – wspólnie z Danielem Wicentym);
- redaktor 4 tomów zbiorowych; autor 15 artykułów w języku polskim i angielskim oraz 7 recenzji;
- od 2007 roku członek rady redakcyjnej „Polish Sociological Review".