

REFLEKSJE WOKÓŁ PRYWATNOŚCI I AUTONOMII INFORMACYJNEJ W ŚWIECIE INTERNETU (WSZECH)RZECZY

Michał Bąba

Wydział Prawa i Administracji Uniwersytetu Opolskiego
ul. Katowicka 87a, 45-060 Opole

Internet (wszech)rzeczy (IoE) wypełnia każdą dziedzinę życia jednostki. Każda sfera prywatności jest podłączana do sieci w zasadzie na stałe. Prywatność, podobnie jak urządzenia podłączone do IoE, zaczyna cechować jednoznaczna identyfikowalność. Fundamentem autonomii informacyjnej jako zasady jest możliwość sprawowania przez jednostkę kontroli nad ujawnianą informacją. Podłączenie do sieci oznacza natomiast stały i automatycznie generowany przepływ danych odbywający się poza świadomością zainteresowanego. Ta antynomia zagraża autonomiczności informacyjnej jednostki. Dążenie do absolutnego odszyfrowania osobowości (do deanonimizacji) rodzi niebezpieczeństwo utraty przez jednostkę kontroli nad informacją. Celem artykułu jest ustalenie, na ile jednostka, uwikłana w proces wymiany danych, jest autonomiczna, co decyduje o jej autonomiczności, czy w środowisku IoE jest ona w ogóle możliwa i jak można ją chronić.

Słowa kluczowe: informacja, dane, autonomia informacyjna, prywatność, algorytmy, internet rzeczy, internet wszechrzeczy.

1. Internet (wszech)rzeczy

Czy otacza nas jeszcze internet rzeczy (IoT)¹, czy może znajdujemy już się w erze IoE²? Jaki jest stopień zespolenia poszczególnych przejawów egzystencji

¹ „Internet rzeczy to infrastruktura obiektów, osób, systemów i zasobów informacyjnych wraz z inteligentnymi usługami umożliwiającymi przetwarzanie w tej infrastrukturze informacji o świecie fizycznym i wirtualnym oraz stosowne reagowanie”, zob. Kruk (2015), str. 12.

² Kierując się wizją Rajeevena Surima – prezesa koncernu Nokia, internet wszechrzeczy reprezentuje ewolucję, w której dotychczas odizolowane obiekty zdolne są do wzajemnej interakcji, to programowalny świat inteligentnej łączności, w którym wszystko będzie połączone ze wszystkim – miliardy sensorów umożliwią usprawnienie i automatyzację wielu czynności. Łączenie będzie dotyczyć wszystkiego ze wszystkim w jedną sieć, skupiającą w

jednostki z siecią, jak bardzo sieć wniknęła w otaczającą nas rzeczywistość czy jednostka jest w stanie kontrolować proces ujawniania danych jej dotyczących, gdy ujawnianie odbywa się automatycznie i wiąże się z nieustannym (na stałe) rejestrowaniem codzienności i kryjących się za nią zwyczajów jednostki?

Liczba podłączonych do sieci urządzeń rejestrujących i mierzących otaczającą jednostkę rzeczywistość wciąż się zmienia, rośnie wykładniczo, za tą zmianą podążają dane i informacje. IoE obrazuje nieustanny ruch olbrzymiej ilości danych, ich pozyskiwanie służy różnym celom, w zależności od tego kto ma być odbiorcą informacji.

Jednostka wytwarza wokół siebie ogromną ilość danych, swoją aktywnością wzbudza ich ruch, w świecie IoE jego intensywność jest rejestrowana przez algorytmy, jest przez nie stale (w nieskończoność) zapamiętywana, nadają mu one określony porządek poprzez wydobywanie z danych określonego sensu, z którego następnie powstają informacje o jednostce, a z nich z kolei budowana jest wiedza, pozwalająca odszyfrować osobowość jednostki. Siła oddziaływania IoE na otaczającą nas rzeczywistość wynika z jego nieograniczonych możliwości analizy informacji.

IoE znosi odrębność jednostki i umożliwia nieograniczony dostęp do niej dzięki obserwacji różnorodnych stanów osobistych jednostki, ujawnianych przez nią spontanicznie. Prywatność można rozpatrywać w różnych kategoriach, uwzględniać różne jej przejawy i obszary, można wreszcie wskazywać na określone wolności (wartości) cząstkowe, z których się składa, które zarysowują kontury znaczeniowe tego pojęcia, niezależnie jednak od liczby wyróżnianych aspektów, każdy jej przejaw i ona sama jest wypełniona danymi i informacjami, które są, jak celnie ujął to B. Stefanowicz (2017, s. 17), wszechobecne.

Prywatność jest obszarem, w którym określonym informacjom na swój temat nadawana jest przez jednostkę pewna określona wartość. Ze względu na tę wartość jednostka stara się je chronić lub też dzielić się nimi. Ujawnienie danych oraz informacji nie przekreśla ich prywatnego rodowodu, jest ono, podobnie jak ich nieujawnienie, świadectwem przysługującej jednostce autonomii, która przenika na wskroś każdą z wolności cząstkowych prywatności.

Fenomen internetu (wszech)rzeczy zasadza się na tym, że nie odczytuje on tej wartości, nie rozumie znaczenia, jakie informacji przypisuje jednostka, gromadzi i ujawnia dane w oderwaniu od wartości informacji nadanej przez jednostkę. Dane oraz informacja stają się wartością samą w sobie. Gromadząc i przetwarzając dane oraz informacje o jednostce internet (wszech)rzeczy nadaje im swoją (nową) wartość, mierzy je i analizuje swoją miarą, poszukuje i odkrywa głębszy ich sens, ukryty pod powłoką danych i informacji, pod wierzchnią ich warstwą znajduje się obszar, który

internetowej chmurze ludzi, przedmioty, procesy i dane. Wywiad dostępny pod adresem - stan na 10 października 2018 r.: <http://www.wykop.pl/ramka/2090302/czym-jest-i-jak-powstaje-internet-wszechrzeczy>

dla algorytmów stanowi zasadnicze pole ich analizy. Okazuje się więc, że algorytmy na nowo łączą poszczególne granule informacji o jednostce, z chwilą ich zarejestrowania nadana informacji przez jednostkę wartość nie przenika wraz z nimi, nie ma najmniejszego po niej śladu w świecie cyfrowym, pozostaje ona w sferze emocjonalnej jednostki, którą algorytmy i tak są w stanie – w pewnej mierze – wyłuskać z samych tylko zebranych danych. Wartość informacji, nadanej przez jednostkę, to znaczenie jakie danej informacji przypisuje jednostka, to rola jaką informacja ta odgrywa w jej życiu, mieści się w tym również przyczyna tego stanu rzeczy, w ten sposób wartość ta obrazuje pewną ciekawą i osobistą historię o jednostce. Algorytmy nie dość, że potrafią odkryć tę historię, bazując na samej warstwie treściowej danych i informacji, to mogą nadać jej nowy i głębszy sens, mogą odkryć zależności i uwarunkowania, które będą w stanie opisać jednostkę w szerszej perspektywie, pozwalającej uchwycić i zrozumieć także inne przejawy jej egzystencji.

Ujmując rzecz bardziej obrazowo, internet (wszech)rzeczy zakłada istnienie świata opartego na wszytkowiedzącym systemie, który będzie widział i monitorował każdy aspekt życia jednostki, będzie rozumiał i rozpoznawał codzienne nawyki, skłonności, będzie wiedział co jednostka czuje, czego potrzebuje, będzie znał jej poglądy, przewidywał jej zachowania, będzie w stanie monitorować konto bankowe i bicie serca, poziom cukru we krwi, długość snu, poziom aktywności oraz stanu zdrowia. System ten będzie w stanie odkryć takie prawidłowości, których jednostka nigdy by nawet nie podejrzewała, będzie mógł mierzyć „jak ludzie faktycznie się zachowują w życiu prywatnym, zamiast mierzyć ich wypowiedzi na ten temat” (Galloway, 2018, s. 131). Będzie to system wkomponowany w istnienie jednostki, będzie stanowił naturalną przestrzeń dla jej osobowości przeszywającą na wskroś jej życie aż po jego kres. Tajemnica, jeśli w ogóle będzie miała jakiegokolwiek znaczenie, stanie się czymś niezrozumiałym, budzącym podejrzliwość i wzmożone zainteresowanie ujawnieniem tego, co się za nią kryje³. Zagrożenie, jakie jest z tym potencjalnie związane, wiąże się z koniecznością bycia widocznym, dotyczy to w równym stopniu wszystkich przejawów ludzkiej egzystencji. W momencie, w którym prywatność stanie się widoczna, jednostka utraci wolność, możliwość zaś decydowania o życiu osobistym stanie się farsą, pustym sloganem, człowiek zostanie odarty z godności, stanie się kolejną bazą danych, podłączoną do sieci. Pojawia się zatem pytanie, co nam wówczas pozostanie – jedynie wszechobecne informacje.

IoE wymaga nowego spojrzenia na prywatność, by móc właściwie zarysować problem, w pierwszej kolejności należy zbadać oraz ustalić kontury znaczeniowe tego pojęcia, co w efekcie pozwoli rozpoznać jego sedno (rdzeń). Prywatność, jak się okazuje, zbudowana jest na wartości, której IoE nie jest w stanie zaakceptować i którą w naturalny sposób zwalcza, jest ona bowiem niezgodna z jego naturą. Teza badawcza jest następująca: *prywatność jest wrogiem internetu (wszech)rzeczy*.

³ W tekście używam zamiennie zwrotów: IoT, czy też IoE lub po prostu sieć. Każdy z nich, mimo oczywistych różnic, reprezentuje na potrzeby omawianej w artykule problematyki taką właśnie wizję świata.

2. Prywatność

Problematykę prywatności spowija chaos terminologiczny. Prywatność jest pojęciem wewnętrznie złożonym i jednocześnie trudnym do uchwycenia, narażonym przez to na niejednoznaczność i wykazującym *prima facie* właściwości, które nie sposób poddać jednej wyraźnie sformułowanej i zamkniętej definicji, którą można byłoby uznać za poprawną lub przynajmniej standardową. Stan toczącej się dyskusji nad pojęciem prywatności ujawnia bogactwo i różnorodność znaczeń nadawanych temu pojęciu. Ich zakresy są na tyle pojemne i otwarte, że niekiedy utrudniają przez to rozpoznanie, że dotyczą one wciąż tego samego pojęcia. Z debaty o prywatności wyłania się mnogość różnorodnych propozycji (Wujczyk, 2012, s. 69-139), z których każda za kryterium dystynkcji pojęciowej, pozwalające na uchwycenie *differentia specifica* prywatności, wskazuje inną jej cechę lub zespół cech. Jest to pojęcie, jak ujął to M. Safjan, o niejasnych konturach znaczeniowych, Safjan (2007, s. 112).

Prywatność jest jedną z aksjologicznych podstaw i przesłanek porządku konstytucyjnego. W odróżnieniu od godności nie jest wartością transcendentną, pierwotną wobec innych praw i wolności człowieka, lecz stanowi ona „prawą ekspresję godności” (Safjan, 2007, s. 102). Ów paradoks tłumaczy zarazem przyczynę trudno uchwytnych granic tego pojęcia, jego pierwowzór, czy też jego źródło istnieje poza granicami poznania (Hołub, 2013, s. 12); w prawnej ekspresji godności dokonuje się „przekształcenie” owej wartości transcendentnej w pojęcie bardziej uchwytnie i wymierne o niejasnych wprawdzie konturach znaczeniowych, pozwalające jednak na zarysowanie pewnych jego obszarów (a więc nieulotne poznaniu), które wszak dzieli ze swym pierwowzorem wspólny „los” niedefiniowalności.

Prywatność jest opisywana na różne sposoby, przy wykorzystaniu wewnętrznych wartości prawa, takich jak: wolności i tajemnicy komunikowania się (art. 49 Konstytucji RP), samostanowienia informacyjnego (art. 51 Konstytucji RP), zasady nienaruszalności mieszkania (art. 50 Konstytucji RP) stanowiącej jedną z „tradycyjnych wolności człowieka” (Winczorek, 2008, s. 118), wolności wyrażania poglądów, wolności pozyskiwania i ujawniania informacji (art. 54 ust. 1 Konstytucji RP), wolności sumienia (art. 53 ust. 7 Konstytucji RP), wolności decydowania o życiu osobistym, przez wskazanie obszarów życia osobistego (życie prywatne i rodzinne) i towarzyszących im stale wartości czci i dobrego imienia (Art. 47 Konstytucji RP). Cześć i dobre imię są trudno uchwytnie, są one zwykle doświadczane przez jednostkę i łączą się z różnym poziomem wrażliwości jednostki, nie posiadają one jakiś zewnętrznych racji uzasadniających, są bardziej kwestią odczuć jednostki, tego jak siebie postrzega, jaki ma obraz samej siebie i jaki ma do siebie stosunek emocjonalny⁴, jak jest postrzegana przez innych. Prywatność jest opisywana również poprzez pryzmat ochrony każdej z tych wartości z osobna i wszystkich łącznie. W ten

⁴ Wyróżnione elementy zbliżają te wartości do pojęcia godności osobistej zaproponowanego przez A. Rodzińskiego (1968), s. 43-49.

oto sposób prywatność zostaje „przyobleczona w postać fundamentalnego prawa podstawowego *right to privacy*” (Safjan, 2007, s. 115).

Prywatność jest zatem nazwą dla wartości samoistnej o złożonej strukturze i bardzo szerokim zakresie, obejmującą wolności cząstkowe i obszary, w których mogą się one uzewnętrzniać, uwzględniającą przy tym wszystkie wymiary egzystencji człowieka, całą jego złożoność i niejednoznaczność. Prywatność eksponuje dające się wyodrębnić przejawy (sfery – Kopff, 1972, s. 41; stany – Westin, 1967, s. 32; aspekty – Mednis, 2006, s. 44-45; kręgi – Wujczyk, 2012, s. 138) egzystencji człowieka. Posiada ona jednocześnie wiele cech wspólnych z takimi kategoriami jak godność człowieka, wolność, równość czy sprawiedliwość. Zakresy niektórych z tych kategorii do pewnego stopnia pokrywają się ze sobą.

Jest to zatem wartość o podstawowej doniosłości dla życia jednostki, wchłania niejako wolności (wartości) cząstkowe, przyobleczone w określone prawa człowieka, podlegające ochronie, ma odniesienie do różnych przejawów życia człowieka.

Wartości te tworzą kontury znaczeniowe pojęcia prywatności. Ich niejasność oznacza, że wszystkie one razem i każda z osobną nie są zdolne do zbudowania zamkniętej definicji tego pojęcia, pozwalają one jednak na wyróżnienie wspólnego im wszystkim punktu oparcia (istoty) – autonomii (wolności) podmiotu, rozumianej jako obszar wolny od ingerencji zewnętrznej.

Analizując poszczególne wolności, za pomocą których opisuje się prywatność, zauważalna jest również pewna prawidłowość. Otóż żadna z tych wolności nie aspiruje do bycia zasadą naczelną prywatności. Każda z tych wolności jest wartością samą w sobie – każda z nich stanowi odrębnie chronioną wartość prawną, przybierającą postać samodzielnej wolności, każda z nich jest wartością samoistną i niezależną i jednocześnie każda z nich stanowi część autonomii podmiotu, każda z nich dotyczy pewnego wskazanego obszaru, w którym wyraża się dana cząstkowa wolność (możemy tu wyróżnić obszary: komunikacji, kontroli jednostki nad informacją jej dotyczącą, decyzyjności jednostki o życiu osobistym rozumianej w kategoriach samostanowienia podejmowania decyzji osobistych o sobie, wyrażania siebie i osobowościowego rozwoju jednostki).

Jednostka pozbawiona jednej z tych wolności w istocie traci wszystkie pozostałe. Moc tych wolności tkwi więc w wewnętrznej ich jedności, w ich, można by rzec, nienaruszalności, która spaja poszczególne obszary w jedną wspólną im wszystkim aksjologiczną „nadprzestrzeń” określaną mianem prywatności.

Każdy z wymienionych tu obszarów nie ma charakteru absolutnego (bezwzględnego), co oznacza, że ograniczenia prywatności są również wpisane w istotę tego pojęcia i mogą dotyczyć jej wolności cząstkowych. Prywatność można wydedukować z godności. Godność jako wartość transcendentna jest niezmienna, jest bytem jednorodnym, prywatność zaś może być stopniowalna, może podlegać

modyfikacjom ze względu na konieczność ochrony innych wartości „wyższego stopnia”.

Prywatność należy więc postrzegać całościowo jako sumę wolności cząstkowych wzajemnie uwarunkowanych, nie można jej sprowadzać do jednego tylko wymiaru. Owe cząstkowe wolności przyobleczone w postać praw człowieka dają się zrelatywizować do rozmaitych przejawów prywatności jednostki.

Prywatność można więc ujmować w perspektywie wewnętrznej i zewnętrznej. W perspektywie zewnętrznej jest opisywana przez pryzmat autonomii. Wówczas nie ma ona tylko wymiaru obronnego, który ma oddzielać jednostkę od świata zewnętrznego (autonomia rozumiana jako zakaz ingerencji w sferę życia duchowego i fizycznego jednostki), lecz w równej mierze eksponuje także drugą jej stronę, tj. swobodę jednostki w decydowaniu o własnym losie. Autonomia podmiotu, będąca wspólnym punktem oparcia dla wszystkich wolności cząstkowych, obejmuje także swobodę jednostki w kształtowaniu jej stosunków z otoczeniem. W perspektywie wewnętrznej prywatność zaś to pewien określony i pożądaný przez jednostkę stan autonomii psychicznej i fizycznej, w którym może ona samodzielnie decydować o sobie i swobodnie kształtować swoją tożsamość oraz indywidualność.

W tym wzajemnym powiązaniu ujawnia się zasadnicza własność prywatności w ogóle i w każdej z jej przejawów (niezależnie od nazw im przypisywanych) – kontrola jednostki nad informacjami na swój temat. Kontrola nie została wprawdzie wysłowiona wprost w treści art. 47 Konstytucji RP, nie ulega jednak wątpliwości, że istotnym aspektem wolności jednostki jest również możliwość sprawowania kontroli nad ujawnianymi na swój temat informacjami.

Przypisana wolności jednostki kontrola nad informacjami ujawnia niewysłowiony wprost w treści art. 47 Konstytucji RP sposób jej ochrony: „zakaz ingerencji w wolność kształtowania przez jednostkę jej życia osobistego” (Fleszer, 2015, s. 23) - jednostka wolna to jednostka zdolna do kontroli życia osobistego, to jednostka zdolna do kontrolowania przepływu informacji z różnych sfer jej życia osobistego, to jednostka, która posiada „władztwo nad dotyczącymi jej informacjami, niedające się sprowadzić tylko do wyrażenia zgody na rozpowszechnianie tych informacji, ale obejmujące również szczególną ochronę informacji” (Braciak, 2002, s. 358). Sposób ochrony tej wartości został uszczegółowiony m.in. w przepisie art. 51 Konstytucji RP.

Prywatność opiera się więc na autonomii woli podmiotu. Obie te sfery są na gruncie Konstytucji chronione.

Przysługująca jednostce zdolność korzystania z prawa do decydowania o życiu osobistym zapewnia jej możliwość skutecznego przeciwdziałania arbitralnej ingerencji, zapewnia jej bycie podmiotem, a nie przedmiotem decyzji. Jednostka pozbawiona tej zdolności nie jest wolna.

3. Autonomia informacyjna według Konstytucji Rzeczypospolitej Polskiej

Przepis art. 51 Konstytucji RP statuuje tzw. zasadę autonomii informacyjnej, stanowiącą szczególną eksplikację prawa do prywatności (art. 47 Konstytucji) i funkcjonalnie powiązaną z wolnością komunikowania się (art. 49 Konstytucji).

Treść zasady autonomii informacyjnej była w dotychczasowym orzecznictwie TK wielokrotnie precyzowana i obszernie omawiana⁵. W rezultacie co do sposobu rozumienia powołanego przepisu wykształciła się utrwalona linia orzecznicza. Autonomia informacyjna, stanowiąca element ochrony życia prywatnego, oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów⁶. Zasadniczym więc aspektem autonomii informacyjnej, jej fundamentem jest kontrola jednostki nad informacją.

Wymiar wolności informacyjnej jednostki (informacyjne samostanowienie) zależy więc od tego, jak daleko sięga obszar, w którego granicach jednostka ma całkowitą swobodę działania według własnej woli, a także od ilości, rodzaju oraz zakresu czynników powodujących, iż wybór nie może stać się jej udziałem. Zakotwiczone w ustawie żądanie ujawnienia ściśle określonych informacji osobowych nie jest wszak ograniczeniem, które uniemożliwia jednostce dokonywanie wyborów w zakresie informacyjnego samostanowienia w ogóle, lecz jest ograniczeniem, które de facto ułatwia zrozumienie i wyznaczenie zakresu wolnej od ingerencji sfery informacyjnego samostanowienia, w ramach której jednostce przysługuje swoboda wolnego od przymusu działania według własnej woli.

Wolność informacyjna składa się z dwóch jej wymiarów: wolności od nieuprawnionej ingerencji oraz wolności do swobodnego działania w sferze wolnej od dozwolonej prawnie ingerencji. Dwoistość autonomii informacyjnej polega więc na konieczności prowadzenia rozważań, uwzględniających jednocześnie wskazane dwa jej wymiary: wymiar wolności jednostki oraz stanowiących jej niezbędne dopełnienie ograniczeń.

Autonomia informacyjna to zatem taki stan, w ramach którego jednostka ma możliwość sprawowania kontroli nad sposobem ujawnienia informacji jej dotyczących, ma możliwość kontroli zakresu tego, co zamierza ujawnić, jak również

⁵ Np. w wyrokach TK z: 24 czerwca 1997 r., sygn. K. 21/96 (OTK ZU nr 2/1997, poz. 23), 11 kwietnia 2000 r., sygn. K. 15/98 (OTK ZU nr 3/2000, poz. 86), 19 lutego 2002 r., sygn. U 3/01 (OTK ZU nr 1/A/2002, poz. 3), 12 listopada 2002 r., sygn. SK 40/01 (OTK ZU nr 6/A/2002, poz. 81), 20 listopada 2002 r., sygn. K 41/02 (OTK ZU nr 6/A/2002, poz. 83), 20 czerwca 2005 r., sygn. K 4/04 (OTK ZU nr 6/A/2005, poz. 64).

⁶ por. np. wyrok TK z 19 lutego 2002 r., sygn. U 3/01.

tego, komu chce ujawnić określone informacje, oraz kiedy zgodę na ujawnienie chce cofnąć. Jest to zatem pewna autonomiczna sfera, w której następuje uznanie własnej podmiotowości, pozwalającej jednostce osiągnąć zamierzony przeze zeń w danej sytuacji stopień indywidualnej wolności. Autonomia informacyjna stwarza więc możliwość ujawniania własnej tożsamości w oparciu o, co do zasady, wolny wybór.

Wyróżniane w nauce prawa przejawy (kręgi, sfery, elementy) prywatności to w rzeczywistości obszary życia społecznego, w których dokonuje się właśnie poprzez autonomię informacyjną urzeczywistnienie wolności jednostki w jej różnorodnych aspektach.

4. Prywatność i autonomia informacyjna jednostki „własnością” algorytmów?

Jak rozumieć sens i znaczenie autonomii informacyjnej w rzeczywistości, która w coraz to większym stopniu zaczyna przypominać połączoną sieć algorytmów, którym jednostka zaczyna oddawać swoją prywatność i indywidualność, którym w efekcie powierza coraz większą liczbę decyzji i wyborów życiowych, i które wiedzą przez to kim ona jest, jak się czuje i czego chce. W jakim stopniu wpływ na autonomiczność wywiera otoczenie, w którym jednostka funkcjonuje i wyraża siebie, w którym ujawnia swoje zwyczaje?

W zamian za dane na swój temat z różnych sfer prywatności jednostka, często nieświadomie, powierza troskę o własne zainteresowania, aktywności i pragnienia algorytmom, które potrafią przewidzieć przyszłe wybory bazując właśnie na rozpoznawaniu prawidłowości.

Aplikacje mogą w przyszłości manipulować jednostką, wpływając na jej pragnienia i podejmując decyzje za nią. Za przykład może posłużyć aplikacja o nazwie Cortana będąca asystentem wirtualnym opartym na algorytmach sztucznej inteligencji, stworzony przez firmę Microsoft. Aplikacja ta ma możliwość dostępu do wszystkich plików, maili i aplikacji. W ten sposób poznaje użytkownika i służy mu radą, np. że trzeba kupić prezent małżonkowi, może za użytkownika wybrać prezent, zarezerwować stół w restauracji i podpowiedzieć o konieczności zażycia lekarstwa. Przed ważnym spotkaniem biznesowym może ostrzec o wysokim ciśnieniu krwi i za niskim poziomie dopaminy, co może sugerować możliwość popełnienia błędów. Może więc zasugerować, by użytkownik nie wychodził poza wstępne ustalenia i powstrzymywał się od podejmowania jakichkolwiek zobowiązań. W szerszej perspektywie przewiduje się, że Cortany mogą przekształcić się w wyroczni w sprawców, mogą zacząć rozmawiać bezpośrednio ze sobą w imieniu swoich szefów np. by uzgodnić czas i miejsce spotkania. Potencjalny pracodawca może dać znać aplikującemu, by ten nie przesyłał swojego CV, lecz zezwolił jego Cortanie na dokładne przepytanie Cortany aplikującego (Harari, 2018, s. 433-435).

Podobnie rzecz się ma z aplikacją Endomondo i innymi jej podobnymi. W szerszej perspektywie, aplikacje tego typu tworzą dostosowane do samego użytkownika sposoby poprawy własnej biologii, oferując w efekcie indywidualnie skrojone diety, plany treningowe, czy też dużą liczbę danych na temat pojedynczego organizmu (Wróblewski, 2016, s. 9). Dane te umożliwiają spersonalizowanie organizmu, wskazanie jego własnych potrzeb (Wróblewski, 2016, s. 9). Kontrola jest jedną z podstawowych cech tego typu aplikacji. Dzięki urządzeniom i aplikacjom człowiek jest w stanie planować czas snu, dietę, liczbę przebytych kroków, zadania do wykonania na dany dzień (Wróblewski, 2016, s. 10).

Dostęp aplikacji do urządzenia wyposażonego w GPS pozwala na zapisywanie danych lokalizacyjnych właściciela urządzenia, np. trasy treningu, jak również do udostępniania tych informacji w mediach społecznościowych, pozwala na ustalenie miejsca zamieszkania, pory i trasy treningów, pozwala również na odkodowanie uwarunkowań zdrowotnych, możliwości fizycznych, także na nieograniczony transfer wszelkich danych prywatnych, zgromadzonych na urządzeniu mobilnym, które nie mają jakiegokolwiek związku z informacją, do której dostęp jest oferowany użytkownikom. W ten sposób uzyskuje się dostęp do informacji behawioralnych, generowanych na podstawie dostępu do danych o używanych aplikacjach i przeglądanych stronach, jak również fizycznej lokalizacji użytkownika w określonym czasie.

W jakim celu aplikacja ujawnia potrzebę dostępu do multimediów, zdjęć, filmów, wiadomości tekstowych sms i innych danych zapisanych na telefonie lub które telefon stale generuje, dlaczego dostęp ten traktuje jako konieczny, niezbędny wręcz warunek korzystania z usługi?

W efekcie zasadniczym celem działania aplikacji nie jest informacja generowana dla użytkowników, korzystających z aplikacji - ta informacja ma zachęcić użytkowników do korzystania z urządzenia, lecz głównym jej celem jest dostęp do danych użytkowników zapisanych na urządzeniach mobilnych. Algorytmy umożliwiają powiązanie tych danych ze sobą, odkodowują prawidłowości w zachowaniu, wyrażaniu emocji, myśli, aktywności, służą profilowaniu dzięki dostępowi do aktywności użytkownika w aplikacjach i na stronach www, przede wszystkim zaś zmiernają do jak najgłębszego poznania użytkownika i to wbrew jego woli.

Pod pozorem ułatwień dostępu do rozwiązań, które mają zachęcić do aktywności fizycznej, tworzy się system, pozwalający na pełne i nieograniczone odszyfrowanie osobowości użytkownika dla celów niezwiązanych z oferowaną usługą. Powyższe prowadzi do wniosku, że urządzenia tego typu są przede wszystkim narzędziem do zbierania informacji o planach życiowych, nawykach, a nawet o pochodzeniu lub skłonnościach seksualnych, czy też problemach zdrowotnych

użytkowników⁷. Ilekroć ujawniamy dane osobowe, ilekroć przekazujemy dane na swój temat do sieci, sprawiamy, że autonomia informacyjna „działa” w zasięgu pozbawionych świadomości algorytmów. Sformułowanie o pozbawionych świadomości algorytmach wskazuje na rozwój nowego rodzaj inteligencji, która jest pozbawiona świadomości, a jednocześnie potrafi wykonywać zadania znacznie lepiej od ludzi. Podkreśla się jednocześnie, że wszystkie zadania wykonywane przez algorytmy (komputery) opierają się na rozpoznawaniu prawidłowości, a pozbawione świadomości algorytmy mogą wkrótce prześcignąć w tym aspekcie ludzką świadomość, wykreślając sobie kurs do superinteligencji. Inteligencja zaczyna się oddzielać od świadomości (Harari, 2018, s. 392 i 393).

5. Dążenie do absolutnego odszyfrowania osobowości – widmo deanonimizacji jednostki

IoE wypełnia lub może wypełnić w przyszłości praktycznie każdą dziedzinę życia jednostki. Każdy poziom, czy też składnik prywatności zaczyna być podłączany do sieci w zasadzie na stałe. Poziom samotności, intymności, anonimowości oraz najbardziej skryty i osobisty – psychologicznej bariery przed niepożądaną ingerencją (Westin, 1967, s. 7), każdy z nich z osobna i wszystkie razem są wypełnione wszechobecnym IoT.

IoT powoli zaznacza swoją dominującą obecność w każdej sferze ludzkiej egzystencji. Atrybuty osobowości jednostki nie są tylko jej atrybutami, niezauważalnie stają się one jednocześnie atrybutami sieci, która wykorzystuje informacje z nich płynące dla różnych celów. Niemiecki polityk Martin Spitz założył operatorowi sprawę sądową i uzyskał w jej wyniku dostęp do wszystkich zgromadzonych przez niego danych na swój temat. Okazało się, że w ciągu 6 miesięcy operator 85 000 razy zarejestrował lokalizację polityka, każdą przeprowadzoną przez niego rozmowę, wraz z numerem, z którym się kontaktował, oraz czasem trwania połączenia. Dysponował kompletem metadanych generowanych przez telefon. Wśród zebranych informacji znalazły się również metadane wiadomości tekstowych. Na podstawie tak uzyskanych informacji możliwym było m.in. opracowanie dziennych raportów obejmujących dokładne adresy zebrań ugrupowania politycznego, do które należał użytkownik, można było również opracować wizualizację szlaków jego podróży po całym kraju, zaznaczając na niej każdy wykonany lub otrzymany telefon (Mitnick, Vamosi, 2017, s. 277 – 279).

Wolność jednostki przestaje się wymykać ograniczeniom przestrzennym. Autonomia osobista, zawierająca w sobie swobodę myśli, wyznania, ekspresji oraz pewnych intymnych zachowań zaczyna się ujawniać w przestrzeni IoE. Jednostka stopniowo przestaje być podmiotem odosobnionym od społeczeństwa, co powoduje,

⁷ Zob. informacje ujawnione przez firmę Selectivv dostępne na stronie <http://selectivv.com/opener-festival-2017-uzytownicy-smartfonow-liczbach-infografika/> - stan na dzień 10 października 2018 r.

iż nie sposób dzielić sfer życia osobistego na sferę intymności, sferę prywatności i sferę powszechnej dostępności (Kopff, 1972, s. 6 i następne), albowiem wszystkie te sfery łączy ze sobą płaszczyzna internetu (wszech)rzeczy, w której dostęp do nich staje się niezwykle ułatwiony.

Wskazany tu podział na sfery, czy też poziomy życia osobistego, zakłada, że jednostka sprawuje kontrolę nad tym, co sama zamierza ujawnić, podział ten odnosi się do sytuacji, w której to jednostka ujawnia dane innym, a zatem to, czego nie ujawnia, jest innym nieznanym, mimo, że aktywności jednostki ze sfery intymności również się dzieją, są obecne w życiu jednostki, a zatem jej autonomia osobista rozgrywa się poza ograniczeniem przestrzennym internetu rzeczy. Pragnienia, emocje, czy też doznania jednostka ujawniana przede wszystkim wobec siebie, nie wychodząc poza krąg własnej osobowości. W internecie rzeczy ujawnienie tych pragnień wobec siebie oznacza jednocześnie ich ujawnienie na zewnątrz (algorytmom), własny krąg osobowości jednostki przestaje być sferą znaną tylko jej, staje się sferą dostępną dla algorytmów. Ich nieujawnienie innym, jeśli zadziało się w sieci, stanowi jednocześnie informację o nieujawnionej sferze intymnej jednostki, o jej pragnieniach, upodobaniach, fantazjach – to co nieujawnione stało się informacją na zawsze zapisaną (w nieskończoność).

Fakty związane z jednostką i jej przeżyciami mogą zostać ujawnione dzięki zrozumieniu relacji zachodzących pomiędzy z pozoru różnymi danymi (informacjami), dzięki odczytaniu pewnych prawidłowości, ujawniających się w aktywnościach jednostki, których nie musi ona nikomu komunikować, one po prostu zachodzą, czy też dzieją się w internecie rzeczy dzięki np. odwiedzaniu różnych stron internetowych zawierających intymne treści, ściąganiu filmów o treściach erotycznych, nawiązywaniu relacji intymnych w sieci, itp.⁸ Duchowa sfera intymności zaczyna być uzewnętrzniana w takim samym stopniu jak inne sfery życia osobistego.

Dzieląc się prywatnością z różnych jej sfer (kręgów) z innymi użytkownikami, jednostka dzieli się nią jednocześnie z pozbawionym świadomości algorytmem, który nigdy niczego nie zapomni i który „autonomiczność” jego użytkowników przekuwa na produkt, który można kupić, którym można odpowiednio i w ściśle określonym celu pokierować (Harari, 2018, s. 436), podtrzymując w człowieku przeświadczenie o tym, że to on sam jest sprawcą swoich wyborów. Amazon wykorzystuje algorytmy, które nieustannie badają klienta, a następnie wykorzystują nagromadzoną wiedzę do polecenia mu produktów. Urządzenia Kindle firmy Amazon jest w stanie gromadzić dane na temat użytkowników podczas lektury. Urządzenie takie może kontrolować,

⁸ Dość typowym innym przejawem analogicznej sytuacji jest internetowy zakup, o którym jednostka chciałaby zachować całkowitą poufność, czy to ze względu na kupowany produkt, czy zachowanie elementu niespodzianki, czy wreszcie niepewność, co do trafności zakupu. Jest to bardzo częsty przypadek, obciążony dodatkowo także swoistym czynnikiem emocjonalnym (red.).

którą część książki użytkownik czyta szybko, na której stronie czytanie jest przerywane, a po którym zdaniu całkowicie rezygnuje się z czytania. Wskazuje się, że jeśli urządzenie tego typu zostaną wzbogacone o rozpoznawanie twarzy i czujniki biometryczne, dowiedzą się, jak każde zdanie wpływa na tętno i ciśnienie krwi. Jak powiada Y. N. Harari: urządzenie to będzie wiedziało „co cię bawi, co smuci, a co złości. Wkrótce, gdy ty będziesz czytać książki, one będą czytać ciebie” (Harari, 2018, s. 436). Dane prywatne, którymi użytkownik sieci dzieli się z innymi użytkownikami, tzn. również z systemem przetwarzania danych, służą w efekcie do zbudowania (wytworzenia) produktu, do „uszczenia go na miarę” potrzeb jednostki odkodowanych i zdefiniowanych na podstawie analizy danych, pochodzących z różnych sfer jej prywatności. Produkt rozumiany jest tu szeroko, jako wszelkiego rodzaju usługi, a nie tylko rzeczy ruchome, również jako informacja. Produktem jest również informacja wygenerowana o jednostce, jej potrzebach, pragnieniach na bazie danych pierwotnych. Ten produkt może podlegać dalszym „obróbkom”, by móc wyłuskać w efekcie pożądaną informację, którą będzie można wykorzystać dla ściśle określonego celu, np. pozyskanie zaufania niezdecydowanego wyborcy. Firma Cambridge Analytica przed 2016 r. wykorzystywała dane wydobyte z kont platform społecznościowych milionów Amerykanów, żeby stworzyć „psychologiczny profil” wyborców. Posługiwała się namierzaniem behawioralnym, żeby przekazywać określone, popierające kandydata Donalda Trumpa treści, odpowiadające określonym wyborcom z bardzo osobistych powodów. Model uwzględniający 150 lajków był w stanie opisać danego użytkownika lepiej niż jego żona czy mąż. Przy 300 lajkach model rozumie użytkownika lepiej niż on sam siebie (Galloway, 2018, s.135)⁹.

Pozyskane w ten sposób dane oraz wyinterpretowane na ich podstawie informacje będą służyć dalszemu wykorzystaniu i analizie. Przykładem może być firma Skyhook Wireless oferująca określone informacje, uzyskane na bazie gromadzonych przez siebie danych geolokalizacyjnych. Mogą one dotyczyć takich kwestii jak to, jakie lokalne bary będą cieszyły się największym powodzeniem w określonym dniu i godzinie, ile osób przejdzie koło danego billboardu w danym dniu i o określonej porze czy też, jaka będzie gęstość ludzi w konkretnym obszarze miejskim w danym dniu i godzinie. Do przeprowadzenia tego typu analiz firma wykorzystuje zanonimizowane dane geolokalizacyjne, zebrane z telefonów komórkowych użytkowników korzystających z jej usług w okresie ostatnich dwudziestu czterech miesięcy w każdym z większych miast amerykańskich (Wielki, 2016, s. 213).

Tych danych nie sposób wymazać, algorytmy nie są stworzone do usuwania danych, do ich wymazywania, tylko do ich ciągłego (automatycznego) gromadzenia i ciągłej analizy. Życie prywatne jednostki i to nie tylko w zakresie, w jakim ujawnia dane na swój temat, jest poddawane w istocie ciągłej analizie, której skutki i znaczenie trudno przewidzieć, w której można jednak dostrzec pewną zarysowującą się już

⁹ podobny eksperyment przeprowadzony przez Facebooka opisuje szczegółowo Y. N. Harari (2018), s. 431 i następane.

prawidłowość: nieograniczony liczbowo zakres możliwych konfiguracji analizy danych dotyczących jednostki. Wynika to nie tylko z liczby stale generowanych przez jednostkę informacji na swój temat, ale również ich zawartości, ich rodzaju, wzajemnego związku, sposobu w jakim jednostka komunikuje siebie itp. Prowadzi to również do pewnego interesującego spostrzeżenia: otóż, owe produkty, będące efektem analizy danych, są opracowywane zanim jeszcze jednostka jest w stanie uświadomić sobie, że je chce, zanim jeszcze zdąży pomyśleć, że ich potrzebuje. Jej akty woli, mające za przedmiot konkretny wytwór pochodzący z analizy jej danych, niekoniecznie muszą więc być wynikiem uświadomionego i w pełni autonomicznego zachowania i mogą być odczytywane w sposób deterministyczny – wywołany przez czynnik zewnętrzny, który w niemal niewidzialny sposób wpływa na ludzkie działania, starając się je ukierunkować w ściśle określonym celu.

Jednostka przestaje być odosobniona w swym własnym świecie. Sfera, która jest domeną własnej aktywności jednostki, stopniowo i niezauważalnie zanika. Owa czysto osobista sfera jednostki staje się elementem wielkiego systemu informacyjnego i podobnie jak inne podłączone do niego inteligentne urządzenia spełnia identyczną funkcję – gromadzenia, przetwarzania i wymiany olbrzymiej ilości różnego typu danych. Dane pochodzące z „czysto osobistej sfery” jednostki są ujawniane lub mogą być ujawniane online w czasie rzeczywistym poza wiedzą jednostki i poza jej kontrolą.

6. IP prywatności?

Prywatność, podobnie jak urządzenia podłączone do internetu rzeczy, zaczyna cechować jednoznaczna identyfikowalność, nie posiada ona wprawdzie własnego adresu IP, jednakże adres taki posiadają urządzenia, podłączone do sieci, monitorujące zachowania jednostki w jej czysto osobistym świecie, gromadzące nieustannie dane dotyczące prowadzonych spraw, podejmowanych decyzji, rodzajów więzi personalnych z innymi, jej przeżyć, potrzeb i planowanych działań. Pośrednio, prywatność może więc posiadać wiele adresów IP, odpowiadających liczbie urządzeń rejestrujących przepływ danych z czysto osobistej sfery jednostki.

W Internecie rzeczy prywatność jest stale odczytywana, analizowana, jest znana i zapamiętana. Można by rzec, że internet rzeczy „oddycha” prywatnością milionów podłączonych do niego za pośrednictwem smartfonów, laptopów i tabletów, również czujników na skórze lub w ubraniach, przekazujących dane, na przykład zdrowotne, czy sportowe użytkowników, prywatność jednostek jest dla niego tym, czym dla organizmu ludzkiego bicie serca. Dążenie do jej poznania nie jest niczym szczególnym, niczym nadzwyczajnym, wręcz przeciwnie nadaje przepływowi danych określony sens – służy bowiem swobodnemu krążeniu informacji w oderwaniu od właścicieli danych i zbiorów danych. Przyświeca temu jeden cel: sprowadzenie ludzkiego życia do przepływu danych w następstwie poddawania wartości ludzkich doświadczeń ciągłej ocenie i analizie. Prowadzi to w efekcie do budowania wiedzy o człowieku, jego przeżyciach, potrzebach, o których on sam nawet nie ma jeszcze

pojęcia, z których istnienia nie zdaje sobie jeszcze sprawy. Wzbudza się w człowieku przekonanie co do konieczności ciągłego decydowania w oparciu o dostarczane mu informacje.

W Internecie rzeczy jednostka nie ma poczucia, że jej sfera prywatności jest w jakiś sposób naruszana, zawłaszczana, czy też ograniczana. Jednostka dobrowolnie przenosi swoją prywatność do sfery publicznej, upublicznia ją dzieląc się z innymi, a przede wszystkim z algorytmami, każdym jej aspektem oraz informacjami, której kryją się za tymi danymi, z których istnienia nie zdaje sobie jeszcze sprawy.

To nie internet rzeczy ingeruje w prywatność, to jednostka czyni zeń użytek wykorzystując do tego celu jej czysto osobistą sferę przeżyć, doznań, pragnień oraz potrzeb.

Internet rzeczy nie zasadza się na konflikcie wartości, tylko na ich synergii. Należy jednak zdać sobie sprawę z pewnego, jeszcze być może nieoczywistego, zagrożenia, że internet rzeczy może dążyć (i to czyni) do niejawnego pozyskiwania informacji na skalę dotąd nieznaną – owo dążenie jest zarazem najbardziej znaczącym aspektem jego ukrytego działania. Chodzi bowiem o to, że internet rzeczy interesuje absolutnie wszystko, ale to wszystko, na temat jednostki, nie chodzi bowiem li tylko o monitorowanie jednostki, lecz o „prześwietlenie” jej życia, o zrozumienie mechanizmów, które nim kierują – a wszystkie te historie ukryte są w danych oraz między danymi. Konflikt wartości może się zatem kryć pod powłoką synergii wartości stale wpajanej jej użytkownikom.

Konflikt wartości ujawnia zasadnicze niebezpieczeństwo dla prywatności rozplywającej się w potoku danych, jest nim inwigilacja, możliwość sprawowania kontroli w zasadzie nad wszystkimi aspektami życia jednostki, dobrowolnie ujawnianymi w warstwie synergii wartości, w której nie obowiązują jakiegokolwiek ograniczenia w obszarze komunikowania się, w której obowiązuje wpajana użytkownikom wolność komunikowania się. F. Brunton i H. Nissenbaum celnie zauważają, że dysponujący wiedzą na nasz temat, mają nad nami władzę. Mogą nie przyjąć nas do pracy, nie udzielić nam kredytu, ograniczyć nasze poczynania, odmówić nam schronienia, członkostwa albo edukacji, czy ograniczyć możliwość korzystania z dobrodziejstwa naszego życia, Brunton i Nissenbaum (2016, s. 131-132). Wolność komunikowania się, wolność wymiany danych stanowi przejaw prawa do prywatności, a zatem internet rzeczy jest postrzegany jako sprzymierzeniec wolności jednostki, utrwała w jednostce poczucie wolności dzięki synergii wartości.

W rzeczywistości, jednakże, to nie jednostka komunikuje się, przekazując określone wiadomości, lecz komunikują się podłączone do sieci urządzenia, które przekazują informację o niej.

7. Asymetria relacji autonomii informacyjnej do internetu (wszech)rzeczy

Profilowanie zmienia paradygmat pojęcia prywatności. Dzielenie jej na sfery, poziomy prywatności, wyróżnianie sfery życia osobistego, które ma być pojęciem szerszym niż prywatność, nie przystaje do internetu rzeczy. Jednostka przynosi swoją aktywność oraz kryjące się za nimi informacje o zwyczajach, o swojej codzienności do sieci, oddaje algorytmom świat osobistych doznań, przeżyć i potrzeb. Profilowanie zakłada możliwość wiązania różnych drobnych, czasami niewiele znaczących danych z otaczającej jednostkę codzienności, by zbudować z nich informację o funkcjonowaniu jednostki, o świecie spraw prywatnych, zawodowych, osobistych, rodzinnych, o tym jak jest postrzegana przez innych, jaką cieszy się opinią, w jakie relacje społeczne wchodzi, jakie ma poglądy, czy i jak się one zmieniają, czym się kieruje w życiu, co ma dla niej znaczenie, z kim się spotyka, jak przedstawia się świat jej intymnych doznań i wyobrażeń, czy jest szczęśliwa, jak rozwija się jej życie rodzinne, czy troszczy się o dzieci, małżonka, czym się interesuje, gdzie z chęcią spędza czas, jak się odżywia, czy jest zdrowa, na co choruje, o czym myśli, a nawet i śni itp. Z tych szczegółowych danych układa się konkretny obraz jednostki, jej życie, jej rys psychologiczny, społeczny, etyczny. Wnioski, do których można dojść na podstawie analizy tych danych mogą być dla jednostki zaskakujące, wręcz niekiedy szokujące, niezrozumiałe, nieadekwatne. Mogą one w niej wzbudzić sprzeciw.

Algorytmy posiadają większą wiedzę o jednostce niż ona sama. Dysponują wiedzą o jednostce, która może zaskakiwać, dzięki posiadaniu lub dostępowi do różnych zasobów danych i informacji. Wiedza ta dotyczy lub może dotyczyć niemalże wszystkich zachowań jednostki, zachodzących w różnych sferach jej życia.

Prywatność „rozplywa się” w danych, każdy aspekt życia osobistego ujawniany w oddzielnych, nie powiązanych ze sobą pierwotnie danych, jest następnie „parowany”, wyszukiwanie i łączenie wymaga odczytania i zrozumienia cech wspólnych ukrytych głębiej na poziomie niedostępnym percepcji jednostki – w „DNA” danych. Zrozumienie prawidłowości rządzących ukryciem pozwala wydobyć, a następnie przeprowadzić rozpoznaje na temat cech indywidualnych, osobowościowych jednostki. „DNA” danych o jednostce może również być ukryte „za” danymi lub inaczej „między” danymi – w ten sposób można dotrzeć do historii za danymi. Dzielenie prywatności na sfery, a te z kolei na podsfony, czy też poziomy i wyróżnianie w ramach każdej z nich rodzaju spraw je definiujących jest w świecie internetu rzeczy zbędne, nie ma racji bytu, jest internetowi rzeczy nieznanne.

Życie jednostki zostaje sprowadzone do nieustannej analizy danych na jej temat, zarówno pod względem ich poprawności (autentyczności), jak i ich przydatności.

Internet rzeczy (algorytmy) uzyskuje władztwo nad prywatnością jednostki z chwilą, gdy okaże się ona przydatna, gdy jej przydatność zostanie potwierdzona i da

się ją wykorzystać. Tak długo, jak długo algorytm nie jest w stanie wyłuskać o jednostce przydatnych informacji na temat jej przyzwyczajzeń, zachowań, więzi, relacji, potrzeb, tak długo, jak długo nie jest w stanie odnaleźć prawidłowości i ma problemy z prognozowaniem jej zachowań, tak długo jednostka zachowuje swoją prywatność. Co się na nią składa? W świecie internetu rzeczy nie ma to znaczenia. Znaczenie ma wyłącznie to, na ile ujawniane o jednostce dane mogą okazać się przydatne do zbudowania wiedzy o jej życiu.

To co w świecie offline nie mieści się w sferze prywatnej, może być uznane za prywatne w świecie online dzięki wydobyciu z nieprywatnych danych prawidłowości na temat jednostki, jej zachowań, potrzeb itp. Dane spoza sfery prywatnej w świecie offline, w świecie online mogą umożliwić prognozowanie zachowań, w świecie online dane te mogą być łączone z danymi ze sfery prywatnej celem odkrycia dalszych interesujących korelacji w postępowaniu jednostki. W świecie online, w świecie internetu, rzeczy prywatność może być więc budowana z danych o jednostce, niezależnie od tego, skąd te dane pochodzą, w której z tych sfer powstały i dlaczego. Każda taka dana może posłużyć do poznania człowieka.

Zainteresowanie budzi tu bowiem absolutnie wszystko, łączenie, kojarzenie, parowanie danych jako następstwo ich przetwarzania, nadaje prywatności inny nieznanym dotychczas wymiar. Inna jest jej skala w świecie Internetu rzeczy. Prywatność to nie tylko sfery, z których jest zbudowana w świecie offline, to również informacja pozwalająca nadać jej, jej sferom, określone i dotąd nieznanie znaczenie, z którego czerpać mogą inni.

Regulacje konstytucyjne mają na celu zachowanie równowagi pomiędzy sferą prywatną i zainteresowaniem sfery publicznej na jej temat. Wymogiem zachowania równowagi jest jasno wytyczona podstawa ingerencji. Równowaga ta nie występuje w świecie internetu rzeczy, który nie żąda od większości danych, „on” je po prostu „dostaje”.

Nierównowaga ta stawia nielicznych (mających dostęp do algorytmów lub informacji przez nie wygenerowanych) w sytuacji uprzywilejowanej wobec absolutnej większości, skazanej na bycie przedmiotem decyzji, które statystycznie się sprawdzają, co do których nie ma jednak pewności, dlaczego zostały podjęte i wcielone w życie. Większość podejmuje zatem decyzje, lub może je podejmować, w warunkach nieświadomego mechanizmu, wynikającego z poddania asymetrii informacji pełnej kontroli nielicznych (algorytmów), wzmacnianej poprzez ukrywanie dostępu do informacji, dezinformację, odwracanie uwagi czy sterowanie decyzjami. W wyniku dystrybucji informacji o jednostce, różne podmioty uzyskują różne informacje. Jednostka uzyskuje np. informacje o produkcie, który może ją zainteresować, o usługach, z których chce skorzystać, algorytm zaś informacje o jej życiu i wzorcach zachowania – jej profil psychologiczny. Efekt dominacji algorytmów (sieci przetwarzających dane) nad jednostką jest oczywisty. Arbitralna „ingerencja” w sferę prywatności cechuje internet rzeczy. Jednostki poddawane są woli i osądowi pozbawionych świadomości algorytmów (nielicznych).

8. Wnioski

Zasada proporcjonalności nie obowiązuje w internecie (wszech)rzeczy. Podłączone do sieci urządzenia monitorujące codzienne zwyczaje jednostki pozyskują dane osobowe bez jakichkolwiek ograniczeń, stawianych władzy publicznej oraz innym podmiotom.

Internet (wszech)rzeczy nie dzieli życia osobistego jednostki na sfery, czy też poziomy, podział ten jest dla sieci nieistotny, albowiem monitorując codzienne zwyczaje jednostki, uzyskuje się dostęp do danych nie tyle o konkretnej sferze prywatności, lecz o życiu osobistym jednostki w ogóle.

Synergia wartości internetu (wszech)rzeczy jest tylko pozorna, oparta jest ona w rzeczywistości na asymetrii informacji, na zdominowaniu jednostki przez system wszystkowiedzących algorytmów, przetwarzających nieustannie dane na jej temat. Zdominowanie jest głęboko ukryte, nie jest w ogóle odczuwalne, jest prawie że niewidoczne, niemalże niezauważalne, faktycznie zaś przenika na wskroś architekturę internetu (wszech)rzeczy, wypełniając każdy element jego ekosystemu.

Prawo do „niebycia z innymi” i „niedzielenia się z innymi” nie istnieje w świecie internetu (wszech)rzeczy. Prywatność nie jest chroniona.

Problem dotyczy nie tego, czy jednostka ma prawo do sprawowania kontroli nad informacją na swój temat, lecz tego, czy systemy przetwarzania danych są zdolne do usunięcia na zawsze danych lub informacji na żądanie jednostki. Czy można unicestwić dane, które w świecie cyfrowym są zapisane (istnieją) w nieskończoność? Co jednak z informacjami przetworzonymi na podstawie analizy danych, które opisują zachowania, emocje, pragnienia, przyzwyczajenia, właściwości zdrowotne jednostki, o których jednostka nigdy nie informowała bezpośrednio, których nigdy nie ujawniła wprost, które są ukryte w informacji – stanowiącej efekt analizy przetwarzania danych pierwotnych. Tych informacji nie sposób ani poznać, ani też ustalić, czy zostały wygenerowane, kiedy i przez kogo, do jakich celów oraz gdzie mogą się znajdować. Usunięcie danych pierwotnych niczego nie zmienia, ponieważ są one zapisane w informacji, których istnienia się nie domyślamy. Cofnięcie zgody na przetwarzanie danych nie usuwa danych na zawsze, albowiem dane te, chociażby pod postacią informacji, wciąż uczestniczą w wielkim przepływie danych.

Gdyby analizować prywatność i autonomię informacyjną z punktu widzenia zdolności jednostki do sprawowania kontroli nad ujawnionymi danymi oraz informacjami, to należy postawić tezę, że autonomia utraciła lub też sukcesywnie traci swój zasadniczy atrybut – kontrolę jednostki nad informacjami na swój temat.

Bibliografia¹⁰

- Braciak J. (2002) Prawo do prywatności. W: B. Banaszak, A. Preisner, red., *Prawa i wolności obywatelskie w Konstytucji RP*. Warszawa.
- Bruton T., Nissenbaum H. (2017) *Zmył trop. Na barykadach prywatności w sieci. Przewodnik*. Warszawa, Wydawnictwo Naukowe PWN.
- Fleszer D. (2015) Godność i prywatność osoby w świetle Konstytucji Rzeczypospolitej Polskiej. *Roczniki Administracji i Prawa* **XV** (1), 23.
- Galloway S. (2018) *Wielka czwórka, four, Ukryte DNA: Amazon, Apple, Facebook, i Google*, Poznań.
- Harari Y. N. (2018) *Homo deus. Krótka historia jutra*. Kraków.
- Hołub G. (2013) *Godność osobowa dziecka nienarodzonego*. W: J. Dziedzic, P. Guzdek, red., *Od bólu po stracie do nadziei życia. Pogrzeb dziecka poronionego*. Wydawnictwo Naukowe Uniwersytetu Papieskiego Jana Pawła II, Kraków.
- Kopff A. (1972) Koncepcja prawa do intymności i do prywatności życia osobistego (zagadnienia konstrukcyjne). *Studia Cywilistyczne*, **XX**.
- Kruk T. J. (2015) Internet rzeczy – rzecz o analizie ryzyka. W: G. Szpor (red.), *Internet rzeczy. Bezpieczeństwo w Smart city*, Warszawa.
- Mednis A. (2006) *Prawo do prywatności a interes publiczny*. Kraków.
- Mitnick K., Vamosi R. (2017) *Niewidzialny w sieci. Sztuka zacierania śladów*. Bielsko-Biała.
- A. Rodziński (1968) U podstaw kultury moralnej. *Roczniki Filozoficzne* **XVI**, 2.
- Safjan M. (2007) *Wyzwania dla państwa prawa*. Warszawa.
- Stefanowicz B. (2017) O analizie informacji. *Zeszyty Naukowe Wydziału Informatycznych Technik Zarządzania Wyższej Szkoły Informatyki Stosowanej i Zarządzania „Współczesne problemy zarządzania”* 2, 7.
- Surima Rajeeven (2018) Wywiad dostępny pod adresem - stan na 10 października 2018 r.: <http://www.wykop.pl/ramka/2090302/czym-jest-i-jak-powstaje-internet-wszechrzeczy>
- Westin A. (1967) *Privacy and Freedom*. New York.
- Wielki J. (2016) Internet rzeczy i jego wpływ na modele biznesowe współczesnych organizacji gospodarczych. *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, 208.
- Winczorek P. (2008) *Komentarz do Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa.

¹⁰ Poza Konstytucją RP, wielokrotnie w tekście przywoływana.

- Wróblewski M. (2016) Nowe szaty healthismu. Self-tracking, neoliberalizm i kapitalizm kongnitywny. *Acta Universitatis Lodzianis, Folia Sociologica* 58.
- Wujczyk M. (2012) *Prawo pracownika do ochrony prywatności*, Warszawa.

REFLECTIONS ON PRIVACY AND INFORMATION AUTONOMY IN THE WORLD OF INTERNET OF (EVERY)THING(S)

Preliminary remarks

Michał Bąba

The Internet of Everything (IoE) fills every area of the individual's life. Every sphere of privacy is connected to the network on a rather permanent basis. Privacy, like devices connected to the IoE, begins to have unambiguous traceability. The foundation of information autonomy as a principle is the ability of the entity to control the disclosed information. Connecting to the network means a constant and automatically generated flow of data taking place outside the consciousness of the interested party. This antinomy threatens the informational autonomy of the individual. The pursuit of absolute deciphering personality (for deanonymization) gives rise to the danger of losing control of the information by the individual. The aim of the article is to determine to what extent the unit entangled in the data exchange process is autonomous, what exactly determines its autonomy, whether it is even possible in the IoE environment and how it can be protected.

Keywords: information, data, information autonomy, privacy, algorithms, internet of things, internet of everything