

Agnieszka Kukla

Tajność i jawność w kontekście ochrony informacji

Według Georga Simmla dzięki tajności dysponujemy drugim światem, który istnieje obok naszego świata jawnego¹. Tajemnica jest nieodłącznym elementem ludzkiego życia. Większa część naszej rzeczywistości psychicznej pozostaje w ukryciu. Z drugim człowiekiem dzielimy się tylko jej fragmentem. Jak pisze Simmel: „Niepodobna wyobrazić sobie kontaktów czy społeczeństwa, które nie opierałoby się na tej – podporządkowanej kategoriom celowości – niewiedzy jednej jednostki o drugiej. To oczywiste, aprioryczne, niejako absolutne założenie obejmuje całą gamę różnic: od szczerzej otwartości po kłamliwą skrytość”². Natomiast według Jacques’a Derridy odebranie prawa do tajemnicy jest drogą do totalitaryzmu³.

Z tajemnicą stykamy się na co dzień. Do przestrzegania szeregu tajemnic obligują nas przepisy prawa lub nasza tajemnica

Agnieszka Kukla – doktorantka Interdyscyplinarnych Humanistycznych Studiów Doktoranckich na Uniwersytecie Warszawskim. Zajmuje się dyskursem politycznym, socjologią komunikacji, filozofią dialogu oraz komunikacją w biznesie.

¹ G. Simmel, *Socjologia*, przeł. M. Łukasiewicz, Państwowe Wydawnictwo Naukowe, Warszawa 1975, s. 412–413.

² *Ibidem*, s. 3.

³ „Według mnie postulat całkowitej jawności sfery publicznej oraz oczekiwanie, że [w sferze tej] nie powinno być żadnych wewnętrznych, niejawnych dyskusji [*internal forum*] stanowi oczywisty symptom totalitaryzacji demokracji. W świetle etyki politycznej można to ująć następującymi słowami: jeśli prawo do tajemnicy nie jest zachowane, to znajdujemy się w totalitaryzmie”. J. Derrida, M. Ferraris, *A Taste for the Secret*, przeł. G. Donis, red. G. Donis, D. Webb, Polity Press, Cambridge 2001, s. 59.

jest przedmiotem ochrony. Prawo chroni tajemnicę zawodową, bankową, lekarską, tajemnicę głosowania, komunikowania się, nasze dane osobowe i wiele innych.

Współczesne państwo również ma swoje tajemnice i bardzo duże potrzeby informacyjne. Ogromne bazy danych są niezbędne do realizowania wszystkich zadań państwa, funkcjonowania administracji, utrzymywania stosunków międzynarodowych czy identyfikowania zagrożeń. W przeszłości tajność obejmowała sfery militarną i polityczną. Obecnie rośnie znaczenie ochrony informacji dotyczącej chociażby sfery ekonomicznej. Informacje niejawne to te, które są związane z przetrwaniem państwa – jego suwerennością, niepodległością i zachowaniem terytorium.

W czasach umasowienia informacji, powstawania nowych kanałów komunikacji, zarządzanie informacjami (zwłaszcza niejawnymi) oraz ich ochrona są bardzo istotne z punktu widzenia bezpieczeństwa państwa. Brak zagrożeń terytorialnych nie jest już wystarczający do orzekania o bezpieczeństwie. A i zagrożenia terytorialne – lub ich brak – są zależne, przynajmniej pośrednio, od bezpieczeństwa informacyjnego. Współczesne bezpieczeństwo państwa jest zatem uzależnione nie tylko od bezpieczeństwa ekonomicznego, politycznego, gospodarczego czy militarnego, ale także właśnie od bezpieczeństwa informacyjnego. Zabezpieczenie informacji jest nie tylko niezbędne, lecz również stało się jednym z elementów zarządzania w społeczeństwie wiedzy⁴.

Ochrona informacji zakłada intencję ich ukrycia, nieupubliczniania. Naturalnie więc wpisane są w nią mechanizmy, które uniemożliwią ich ujawnienie. Zarządzanie taką ilością informacji, jaką dysponuje współczesne państwo, implikuje bardzo wiele pytań: o to, czy regulacje w zakresie bezpieczeństwa informacyjnego są aktualne i adekwatne, czy dysponujemy odpowiednimi narzędziami ochrony, jak głęboka powinna być ingerencja pań-

⁴ S. Zalewski, *Współczesne państwo i jego tajemnice*, w: *Przeszłość, teraźniejszość i przyszłość. Ochrona informacji niejawnych w zapewnieniu bezpieczeństwa narodowego*, red. J. Sobczak, Krajowe Stowarzyszenie Ochrony Informacji Niejawnych; Uniwersytet Śląski, Wydział Informatyki i Nauki o Materiałach, Katowice 2014, s. 37–52.

stwa w prywatność obywateli, służąca zapewnieniu bezpieczeństwa. Mając na uwadze te pytania, postaram się przybliżyć chociaż kilka kontekstów tajności i jawności w aspekcie ochrony informacji. Na początku zajmę się rosnącą rolą informacji w społeczeństwie informacyjnym. Następnie omówię trzy perspektywy tajności i ochrony informacji. Pierwszą jest ochrona informacji z perspektywy państwa i temu poświęcę kolejną część tekstu. Druga – to perspektywa obywatela i tutaj chciałabym zwrócić uwagę na to, jakie gwarancje bezpieczeństwa danych mamy jako obywatele, a także jak historycznie zmieniło się postrzeganie sfer publicznej i prywatnej oraz autonomii informacyjnej. Trzecią perspektywą jest perspektywa relacji między obywatelem i państwem.

Rola informacji i społeczeństwo informacyjne

Termin „społeczeństwo informacyjne” został wprowadzony przez japońskiego antropologa Tadao Umesao w 1963 roku. Zyskał na popularności po tym, jak Kenichi Koyama użył go w rozprawie *Introduction to Information Theory* (1968). W Europie i Stanach Zjednoczonych upowszechnił się w latach osiemdziesiątych.

W klasycznym ujęciu Daniela Bella to właśnie wiedza i informacja były determinantami przemian społecznych w społeczeństwach postprzemysłowych. Tomasz Goban-Klas i Piotr Sienkiewicz definiują społeczeństwo informacyjne jako społeczeństwo, które „nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz przetwarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa”⁵.

Jesteśmy z reguły zgodni co do tego, że żyjemy obecnie w społeczeństwie informacyjnym. Informacja stała się już wartością samą w sobie. Człowiek jeszcze nigdy w swojej historii nie przesyłał,

⁵ T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne. Szanse, zagrożenia, wyzwania*, Wydawnictwo Fundacji Postępu Telekomunikacji, Kraków 1999, s. 53.

nie gromadził i nie przetwarzał tak ogromnej liczby danych. Informacja jest najpewniej najważniejszym niematerialnym czynnikiem przemocy oraz środkiem przymusu. Skuteczne narzędzia i umiejętności gromadzenia, przetwarzania oraz analizowania informacji stanowią o konkurencyjności. Według Manuela Castellsa „Produktywność i konkurencyjność w produkcji informacyjnej (*informational production*) opierają się na wytwarzaniu wiedzy i przetwarzaniu informacji. Wytwarzanie wiedzy i możliwości technologiczne są kluczowymi środkami konkurencji dla firm, organizacji wszelkiego rodzaju, a wreszcie krajów”⁶.

Zmiany technologiczne implikują przeobrażenia w procesie przetwarzania informacji. Mają wpływ na wszystkie obszary aktywności ludzi. Dzięki nowym technologiom możemy tworzyć niczym nie ograniczone powiązania między sferami, podmiotami i elementami tej aktywności⁷.

Wiedza, która jest powiązana z informacją, jest też bardzo często ekskluzywna. Podobnie jak ekskluzywna bywa tajemnica. Jedno i drugie jest też nieodłącznie kojarzone z władzą. Jak zauważa Michel Foucault: „władza i wiedza wprost się ze sobą wiążą [...] nie ma relacji władzy bez skorelowanego z nimi pola wiedzy, ani też wiedzy, która nie zakłada i nie tworzy relacji władzy”⁸.

Wszystkie wielkie korporacje gromadzą informacje dotyczące swoich klientów i wykorzystują je w celach marketingowych. Dotyczy to właściwie każdej branży – finansowej, telekomunikacyjnej czy sfery prywatnej opieki medycznej. Gromadzenie i przetwarzanie informacji jest jednym z najważniejszych zadań przedsiębiorstw, które chcą generować większe zyski. Dane osobowe, które już zostały pozyskane, mogą jednak być wykorzystywane niezgodnie z pierwotnymi celami. Sprzedaż danych osobowych stała się już odrębną gałęzią handlu, mimo że w bardzo wielu

⁶ M. Castells, *Spółeczeństwo sieci*, przeł. M. Marody, K. Pawluś, J. Stawiński, S. Szymański, Wydawnictwo Naukowe PWN, Warszawa 2013, s. 150.

⁷ *Ibidem*, s. 110.

⁸ M. Foucault, *Nadzorować i karać. Narodziny więzienia*, przeł. T. Komendant, Wydawnictwo Aletheia, Warszawa 1993, s. 34.

przypadkach jest nielegalna. Na podstawie zgromadzonych danych tworzy się profile psychologiczne, kreuje potrzeby konsumpcyjne, buduje strategie marketingowe, odpowiednio adresuje kampanie reklamowe czy nawet profiluje posprzedażową obsługę klienta. Tomasz Goban-Klas i Piotr Sienkiewicz zwracają uwagę, że tworzenie baz danych i profili psychologicznych „to podstawa strategii perswazyjnych, ale może być także podstawą kontroli społecznej i indywidualnej”⁹.

Bezpieczeństwo informacji w państwie

Rozwój nowoczesnego państwa wiąże się ze wzrostem roli informacji. Szybki dostęp do pewnej i sprawdzonej informacji, a także umiejętność jej przetworzenia, są warunkiem skutecznego działania państwa. Z drugiej strony niezabezpieczenie posiadanych informacji może stanowić zagrożenie dla bezpieczeństwa państwa. Dlatego zapewnienie bezpieczeństwa informacyjnego jest jednym ze strategicznych zadań państwa. Czym jest bezpieczeństwo i bezpieczeństwo informacyjne?

Trudność w zdefiniowaniu bezpieczeństwa jest wynikiem między innymi tego, że bezpieczeństwo jest zagadnieniem interdyscyplinarnym. Dlatego nie ma jego jednej, wspólnej definicji. Można je rozumieć jako stan, proces lub potrzebę i wartość. Bezpieczeństwo jest definiowane jako stan przez Waldemara J. Wołpiuka, według którego „[...] o bezpieczeństwie możemy mówić zwłaszcza wówczas, gdy w jakiejś dziedzinie ma miejsce stan braku zagrożenia, zaufania spokoju i pewności. Jeśli zważymy, że bezpieczeństwo jest oceniane – jako pewien stan – z punktu widzenia czynników subiektywnych i obiektywnych, to stan bezpieczeństwa istnieje wówczas, gdy subiektywne i obiektywne czynniki wskazują na brak zagrożenia bezpieczeństwa. Natomiast gdy istnieje zarówno wysoka i obiektywna niepewność braku zagrożenia, gdy

⁹ T. Goban-Klas, P. Sienkiewicz, *Spółczesność...*, s. 58.

istnieją również obiektywnie stwierdzone przejawy rzeczywistego zagrożenia, a także gdy istnieją subiektywnie postrzegane czynniki świadczące o zagrożeniu, wówczas możemy stwierdzić, że występuje stan braku bezpieczeństwa. Państwo, jego terytorium, władze publiczne, człowiek, stosunki społeczne (i inne) są bezpieczne, gdy są niezagrożone¹⁰. W tej perspektywie bezpieczeństwo jest zatem stanem, sytuacją, w której mamy całkowitą pewność braku zagrożenia, a na ten brak wskazują czynniki zarówno subiektywne, jak i obiektywne. Nawet subiektywne poczucie zagrożenia będzie więc oznaczało stan braku bezpieczeństwa.

Zgodnie z perspektywą procesualną bezpieczeństwo będzie rozumiane jako nieustająca aktywność jednostek, grup czy wreszcie państw i wspólnot ponadnarodowych. Mówiąc innymi słowy: bezpieczeństwo to ciągle reagowanie, a organizacja bezpieczeństwa to zarządzanie zmianą, uzależnione od kontekstów i uwarunkowań¹¹.

Jerzy Jaskiernia proponuje następującą definicję: „Bezpieczeństwo jest procesem, w którym ścierają się funkcjonujące wyzwania i zagrożenia, percepcja społeczna i koncepcje ich rozwiązania oraz działania i oddziaływania państw i instytucji międzynarodowych, zmierzające do budowania ich pewności przetrwania, posiadania i swobód rozwojowych”¹².

Bezpieczeństwo rozumiane jako proces podlega zatem dynamicznym zmianom, na które mają wpływ zachowania, postawy, postrzeganie sytuacji społecznej czy aktywności instytucji na poziomie narodowym i ponadnarodowym.

¹⁰ W.J. Wołpiuk, *Bezpieczeństwo państwa i pojęcia pokrewne. Aspekty konstytucyjnoprawne*, w: *Krytyka prawa. Niezależne studia nad prawem*, t. 2: *Bezpieczeństwo*, red. W. Sokolewicz, Warszawa 2010, s. 183. Cyt. za: W. Lis, *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, Wydawnictwo Katolickiego Uniwersytetu Lubelskiego, Lublin 2015, s. 33.

¹¹ W. Pokruszyński, *Filozoficzne aspekty bezpieczeństwa*, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej, Józefów 2011, s. 10.

¹² J. Jaskiernia, *Bezpieczeństwo państwa a ochrona praw i wolności jednostki w Polsce – obszary koegzystencji i konfliktu tych wartości w kontekście realizacji standardów międzynarodowych i wewnętrznych*, w: *Bezpieczeństwo państwa a ochrona praw i wolności jednostki we współczesnym świecie*, red. *idem*, Wydawnictwo Uniwersytetu Jana Kochanowskiego, Kielce 2012, s. 49.

Podejście aksjologiczne zakłada, że bezpieczeństwo jest jedną z najważniejszych wartości w ludzkim życiu. Jak stwierdza Waław Kubies: „Bezpieczeństwo należy traktować jako wartość nadrzędną, skupiającą w sobie wszystkie inne wartości”¹³. Perspektywę aksjologiczną znajdziemy też u Jana Szmyda: „bezpieczeństwo jest wartością wysoko usytuowaną w hierarchii wartości ze względu na swoją wagę i znaczenie dla każdego człowieka, ale będącą jednak wartością nieautoteliczną, nie samą w sobie, to znaczy nie godną zabiegów ze względu na nią samą, natomiast wartością wyraźnie użyteczną, użytkową, to znaczy będącą środkiem do osiągnięcia (zabezpieczenia) innych wartości, np. życia, zdrowia, własności”¹⁴.

Bezpieczeństwo w tej perspektywie jest zatem wartością, w dodatku wartością nadrzędną lub umiejscowioną bardzo wysoko w hierarchii wartości. Dzięki bezpieczeństwu możliwe jest osiąganie innych wartości – zarówno tych materialnych, jak i duchowych. Bezpieczeństwo jako wartość nierozzerwalnie łączy się z jakością życia, realizowaniem celów czy zabezpieczeniem praw.

Szmyd zwraca również uwagę na ważną cechę bezpieczeństwa jako wartości – bezpieczeństwo nie jest ważne ze względu na nie samo. Ustanowienie normatywnych regulacji dotyczących bezpieczeństwa wymaga określenia jego przedmiotu lub podmiotu. Dopiero selekcja kategorii bezpieczeństwa (na przykład bezpieczeństwo osobiste) pozwala na to, żeby stały się one elementami regulacji¹⁵.

Przez bezpieczeństwo państwa należy rozumieć ochronę przed zagrożeniami militarnymi, ekonomicznymi czy gospodarczymi. Zapewnienie bezpieczeństwa państwa wymaga ochrony informacji

¹³ W. Kubies, *Poczucie bezpieczeństwa w aspekcie bezpieczeństwa państwa*, w: *Bezpieczeństwo – powinność czy gwarancja. Prawa i wolności a działanie państwa*, t. 3, red. T. Miłkowski, Oficyna Wydawnicza „Humanitas”, Sosnowiec 2015, s. 53.

¹⁴ J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, w: *Zarządzanie bezpieczeństwem. Międzynarodowa konferencja naukowa, Kraków 11–13 maja 2000*, red. P. Tyrała, Kraków 2000, s. 48, cyt. za: W. Lis, *Bezpieczeństwo...*, s. 33.

¹⁵ W.J. Wołpiuk, *Bezpieczeństwo państwa a prawo do wolności i bezpieczeństwa osobistego*, w: *Bezpieczeństwo państwa...*, s. 87.

istotnych z punktu widzenia jego funkcjonowania. Systematycznie wzrasta świadomość tego, jak ważna jest ochrona informacji dla interesów gospodarek narodowych. Bezpieczeństwo informacyjne jest definiowane na wiele sposobów. Małgorzata Plecka i Anna Rychły-Lipińska definiują bezpieczeństwo informacyjne między innymi jako ogół procesów, w których informacje są generowane i przetwarzane; zapewnienie tajności, spójności i niezawodności działań, które są związane z przetwarzaniem i udostępnianiem informacji; stan, który gwarantuje państwu swobodę i rozwój społeczeństwa informacyjnego czy ochronę informacji niejawnych¹⁶. Bezpieczeństwo informacyjne państwa jest realizowane poprzez zabezpieczenie zasobów informacyjnych i infrastruktury.

Szczegółnej ochronie podlegają informacje niejawne. Zaliczamy do nich informacje: (a) ściśle tajne, których ujawnienie może spowodować wyjątkowo dużą szkodę dla państwa, między innymi w zakresie ochrony suwerenności, porządku konstytucyjnego czy relacji międzynarodowych; (b) informacje poufne, czyli takie, których ujawnienie może spowodować szkodę, na przykład zakłócając porządek publiczny lub utrudniając prowadzenie bieżącej polityki; (c) informacje zastrzeżone – ich ujawnienie może mieć szkodliwy wpływ na wykonywanie zadań przez organy władzy i administrację publiczną, bezpieczeństwo publiczne czy wolność obywateli¹⁷.

Według Sławomira Zalewskiego informacje niejawne możemy scharakteryzować jako „[...] instrument władzy politycznej. Istotą tego ujęcia jest jednak nie tyle analiza prawnych regulacji ochrony informacji niejawnych, ale ich ujęcie w kategoriach instrumentalnych, tj. środka wywierania wpływu w relacjach społecznych. Od wieków tajemnica uchodzi za narzędzie panowania jednego człowieka nad innymi”¹⁸.

¹⁶ M. Plecka, A. Rychły-Lipińska, *Bezpieczeństwo informacyjne*, w: *Wybrane problemy bezpieczeństwa. Dziedziny bezpieczeństwa*, red. A. Urbanek, Wydawnictwo Społeczno-Prawne, Słupsk 2013, s. 165–166.

¹⁷ *Ibidem*, s. 183–184.

¹⁸ S. Zalewski, *Współczesne państwo...*, s. 44.

Nieuprawniony dostęp do informacji niejawnych może stwarzać poważne zagrożenie dla bezpieczeństwa państwa. Dlatego są one chronione przez szereg regulacji, które mają zapobiec ich udostępnieniu osobom nieuprawnionym. Z drugiej strony, w perspektywie przywołanej przez Sławomira Zalewskiego, sam dostęp do informacji niejawnych może skutkować ich wykorzystaniem instrumentalnym, na przykład w celu wywierania wpływu społecznego. Informacja może zatem być wykorzystana jako czynnik przewagi i władzy.

Zagrożenia dla bezpieczeństwa informacyjnego mogą być wynikiem samej natury informacji, jej cech, do których Agnieszka Olechnicka zalicza między innymi: łatwość koncentracji (użytkownik wpływa na objętość informacji), nieodwracalność (rozprzestrzenianie informacji jest jednokierunkowe) oraz katalityczność (informacja określa kierunek działań)¹⁹.

Współcześnie dużym zagrożeniem dla bezpieczeństwa informacyjnego jest cyberterroryzm, który staje się coraz powszechniejszy ze względu na szeroką dostępność sprzętu komputerowego oraz łatwy dostęp do wiedzy i oprogramowania, które taki atak umożliwiają. Cyberprzestępczość to nie tylko atak na systemy informatyczne czy uzyskiwanie dostępu do tajnych informacji. Jej elementem jest także rozpowszechnianie informacji fałszywych albo propagandowych²⁰.

Większość obszarów, w których funkcjonuje współczesne państwo, jest uzależniona od sprawnego funkcjonowania systemów teleinformatycznych oraz ich ochrony. Gromadzenie i przetwarzanie informacji jest niezbędne do wykonywania podstawowych zadań państwa: obronności oraz realizowania polityki społecznej, gospodarczej i ekonomicznej. Zasoby informacyjne są w coraz większym zakresie digitalizowane. Dlatego w dobie społeczeństwa informacyjnego, powszechnej wymiany informacji, zwłaszcza za pośrednictwem środków porozumiewania się na odległość, zapewnienie bezpieczeństwa informacyjnego i teleinformatycznego jest jedno-

¹⁹ A. Olechnicka, *Rozwój regionalny w warunkach gospodarki informacyjnej*, „Studia Regionalne i Lokalne” 2000, nr 4, s. 39.

²⁰ M. Plecka, A. Rychły-Lipińska, *Bezpieczeństwo...*, s. 179–180.

znaczne z ochroną tajemnicy państwa. Ujawnienie tej tajemnicy może powodować szkody we wszystkich sferach jego funkcjonowania, zagrozić bezpieczeństwu państwa i jego obywateli.

Tajność w kontekście prywatności i sfery publicznej

Nie ma jednej definicji prywatności. Według Jana van Dijka prywatność z reguły definiujemy jako „prawo jednostki do decydowania, czy i do jakiego stopnia gotowa jest otworzyć się na innych”²¹. Autor ten przywołuje również drugą definicję, zgodnie z którą prywatność to „prawo do zażądania od innych, aby zostawili nas w spokoju”²². Rozumienie zgodne z tą drugą definicją prawdopodobnie po raz pierwszy zostało wyrażone przez Samuela D. Warrena i Louisa D. Brandeisa w artykule *The Right to Privacy* z 1890 roku. Autorzy ci zdefiniowali prawo do prywatności, wykorzystując sformułowanie sędziego Thomasa Cooleya o prawie do bycia pozostawionym samemu sobie (*the right to be let alone*)²³.

W wąskiej perspektywie prywatność oznacza prawo do zachowania tajemnicy o swoim życiu, to znaczy możliwość utajnienia wybranych informacji na swój temat. Poufność jest prawem jednostki do decydowania o tym, którymi informacjami chce się podzielić z innymi ludźmi oraz które jest skłonna od nich przyjąć. Tajność jest atrybutem danych opisującym stopień ochrony, jakiej mogą one podlegać, uzgadnianym przez osoby lub organizacje otrzymujące te dane²⁴.

Współcześnie prawo do prywatności oznacza: autonomię informacyjną (czyli prawo do decydowania o tym, które informacje

²¹ J. van Dijk, *Společne aspekty nowych mediów*, przeł. J. Konieczny, Wydawnictwo Naukowe PWN, Warszawa 2010, s. 160.

²² *Ibidem*.

²³ S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review” 1890, t. 4, nr 5, s. 193.

²⁴ T. Goban-Klas, P. Sienkiewicz, *Spółczesność...*, s. 73.

na swój temat ujawniamy), ochronę cielesności i życia rodzinnego oraz intymności. W porządku prawnym istnieje wiele regulacji chroniących naszą prywatność. Zgodnie z *Konwencją Rady Europy* nr 108 z 28 stycznia 1981 roku²⁵ informacje na nasz temat mogą być gromadzone tylko legalnie, w celu zgodnym z prawem. Dane wrażliwe nie mogą być przetwarzane automatycznie, a przechowywanie danych, dzięki którym można nas zidentyfikować, jest ograniczone czasowo. Mamy prawo do informacji o tym, że nasze dane są przechowywane, w jakim celu oraz przez kogo. Możemy żądać ich modyfikacji²⁶. Ponadto mamy prawo do „bycia zapomnianym” – możemy zażądać, aby nasze dane usunięto z bazy, zwłaszcza w przypadku, gdy zostały zebrane nielegalnie lub wykorzystane niezgodnie z przeznaczeniem²⁷.

Szczególnej ochronie podlegają nasze dane osobowe, czyli te, na których podstawie można nas zidentyfikować. Katalog takich danych jest otwarty i trudno jednoznacznie określić, które dane należy do nich zaliczyć, ponieważ jest to uzależnione od kontekstu i sytuacji. Nie zawsze podanie jednej danej w określonych okolicznościach będzie umożliwiało zidentyfikowanie osoby. Nie można natomiast wykluczyć zaistnienia kontekstów i sytuacji, w których ta sama dana umożliwi taką identyfikację.

Inaczej jest z danymi wrażliwymi. Są one szczególnie chronione, a ich lista jest zamknięta. Są to dane o naszym pochodzeniu rasowym i etnicznym, przekonaniach religijnych i etycznych, przynależności związkowej, religijnej lub partyjnej, a także dane o stanie zdrowia, kodzie genetycznym, nałogach, życiu seksualnym. W tym samym katalogu znajdują się również informacje o orzeczeniach wydanych w postępowaniu sądowym lub administracyj-

²⁵ *Konwencja nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r.*, „Dziennik Ustaw” 2003, nr 3, poz. 25.

²⁶ M. Pryciak, *Prawo do prywatności*, w: *Prawa człowieka – idea, instytucje, krytyka*, red. M. Sadowski, P. Szymaniec, „Wrocławskie Studia Erazmiańskie” 2010, zeszyt IV, s. 225.

²⁷ A. Mednis, *Prawo do bycia zapomnianym*, „Czas Informacji” 2013, nr 2 (14), za: J. Niklas, *Prywatność w Internecie*, „Infos” 2014, nr 13 (173), s. 3.

nym, o mandatach i karach. Przetwarzanie danych wrażliwych jest możliwe tylko w ściśle określonych warunkach, takich jak na przykład ochrona zdrowia czy dochodzenie praw przed sądem. Dane wrażliwe dotyczą w dużym stopniu sfery naszej prywatności oraz życia intymnego. Mamy prawo do nieujawniania tych danych. Ta sfera naszego życia jest szczególnie chroniona, między innymi dlatego, że nadajemy jej wartość, co wynika również z naszego definiowania i postrzegania sfery publicznej oraz sfery prywatnej. Jeżeli spróbujemy ująć to postrzeganie historycznie, zauważymy, że nasze obecne definicje i perspektywy różnią się od tych, które obowiązywały dawniej.

Hannah Arendt analizowała przeobrażenia, który zaszły w społeczeństwach zachodnich i były przyczyną zmiany w definiowaniu sfer prywatnej i publicznej, a także relacji między nimi. Punktem wyjścia był dla niej podział w ramach *vita activa* na fundamentalne (ponieważ odpowiadające jednemu z warunków życia) aktywności człowieka: pracę, wytwarzanie i działanie. Jak stwierdziła: „Wszystkie trzy czynności i odpowiadające im uwarunkowania są ściśle związane z najogólniejszym warunkiem egzystencji ludzkiej: narodzinami i śmiercią, przychodzeniem na świat, śmiertelnością. Praca zapewnia nie tylko indywidualne przetrwanie, ale i życie gatunku. Wytwarzanie i jego produkt, rzeczy wytworzone przez człowieka [...] nadają ulotności śmiertelnego życia i przemijaniu ludzkiego czasu pewien stopień trwałości stałości. Działanie, angażując się w ustanawianie i ochronę ciał politycznych, stwarza warunki dla pamięci, czyli dla historii”²⁸.

W starożytnej Grecji gospodarstwo domowe i rodzina były sferą prywatną, sferze publicznej natomiast odpowiadało życie polityczne. To, co miało naturę ekonomiczną i było związane z podtrzymywaniem życia było dla Greków niepolityczne. Sfera prywatna była o tyle istotna, o ile umożliwiała funkcjonowanie w sferze publicznej. Była wobec niej podrzędna. Działania służące pod-

²⁸ H. Arendt, *Kondycja ludzka*, przeł. A. Łagodzka, Wydawnictwo Aletheia, Warszawa 2010, s. 27.

trzymywaniu życia lub gatunku postrzegano jako konieczność, a dopiero przestrzeń publiczna była synonimem wolności i tylko tam wolność można było odnaleźć. Sfera prywatna była przedpolityczna, zhierarchizowana i funkcjonowały w niej relacje władzy i rządzenia – zupełnie inaczej niż w *polis*, gdzie wszyscy obywatele byli równi, a tym samym wolni. W sferze publicznej funkcjonowało tylko to, co istotne, to, co przekracza granice życia. Tym samym nie było w niej miejsca na przykład na ból, który został przesunięty do sfery prywatnej. Jedyny wyjątek stanowiła własność. Tylko własność, chociaż należąca do sfery prywatnej, miała wyjątkowy status, ponieważ nadawała miejsce w świecie, ochronę prawną i obywatelstwo.

Zmiana w definiowaniu sfer publicznej i prywatnej, a także relacji zachodzących między tymi sferami, zaczęła się wraz z powstawaniem sfery społecznej. Do jej wyłaniania przyczynił się nowożytny indywidualizm. To, co prywatne ujrzało światło dzienne, podczas gdy w starożytności prywatność była kojarzona z deprawacją. W społeczeństwie to, co jest związane z przetrwaniem, co stanowiło przedmiot tajemnicy, zaczęło się przedostawać do sfery publicznej.

Obecnie na widok publiczny wystawiane są sprawy związane z naszym życiem rodzinnym, cielesnością, seksualnością. Jak zauważył Michel Foucault, nasza seksualność stała się przedmiotem nauki i dyskursów. W *Historii seksualności* czytamy: „Seks, wydobyty z ukrycia, skazany zostaje na istnienie w dyskursie. Od jednostkowego imperatywu, zmuszającego każdego człowieka do poddawania własnej seksualności ustawicznemu dyskursowi, aż po wielorakie mechanizmy, które w obrębie ekonomii, pedagogiki, medycyny, sądownictwa zachęcają, wyodrębniają, porządkują, instytucjonalizują mówienie o seksie, cywilizacja nasza osiągnęła i zorganizowała niebywałe rozgadanie”²⁹.

Ciało funkcjonuje w przestrzeni publicznej. Stało się narzędziem definiowania i konstruowania własnego obrazu społecznego.

²⁹ M. Foucault, *Historia seksualności*, t. 1: *Wola wiedzy*, przeł. B. Banasiak, K. Matuszewski, Czytelnik, Warszawa 1995, s. 36.

Przestało stanowić przedmiot tajemnicy. Według Bryana Turnera ciało możemy postrzegać jako możliwość, która nabiera kształtu istniejąc w kulturze i może być rozwijana w ramach interakcji międzyludzkich³⁰.

Pielęgnowanie ciała, zabiegi, które mają je udoskonalić, stan naszego zdrowia, przestały być przedmiotem tajemnicy, tego, co dawniej stanowiło element sfery prywatnej. Wytyczne, które dotyczą wyglądu i zdrowia ciała, oprócz tego, że są wszechobecne, stały się też na swój sposób obligatoryjne. Odnoszą się do nas wszystkich i wszyscy jesteśmy zobowiązani do ich przestrzegania. Niezgodność z normą oznacza odmienność (żeby nie powiedzieć: wykluczenie). Stan naszego ciała stał się przedmiotem powszechnych dyskursów medycznych, estetycznych, a wreszcie – seksualnych. Ponadto stał się przedmiotem regulacji, a co więcej – jest wykorzystywany instrumentalnie w debacie na temat finansów publicznych, chociażby w zakresie kosztów leczenia chorób, które, w powszechnym rozumieniu, wynikają z niewłaściwego stylu życia. Tym samym to, co prywatne stało się przedmiotem dyskursów i przestrzeni publicznej.

David Lyon w rozmowie z Zygmuntem Baumanem przywołuje pojęcie erozji anonimowości, która jest efektem powszechnego korzystania z serwisów społecznościowych oraz używania telefonów komórkowych wyposażonych w kamery i aparaty fotograficzne. Wszelkie treści zarejestrowane za pomocą tych narzędzi możemy udostępnić innym za pośrednictwem darmowych i dostępnych wszystkim użytkownikom serwisów internetowych. Jest to też efekt zmiany naszego postrzegania tego, co publiczne oraz tego, co prywatne, o czym już wcześniej wspomniałam³¹.

Upublicznianie przez nas samych informacji o sobie można rozumieć po prostu jako indywidualne realizowanie autonomii

³⁰ B. Turner, *Regulating Bodies. Essays in Medical Sociology*, Routledge, New York 1992, s. 16, cyt. za: A. Młynarska-Sobaczewska, *Trzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społecznej*, „Przegląd Prawa Konstytucyjnego” 2013, nr 1 (13), s. 40.

³¹ Z. Bauman, D. Lyon, *Płynna inwigilacja rozmowy*, przeł. T. Kunz, Wydawnictwo Literackie, Kraków 2013, s. 39.

informacyjnej. Oczywiście można to różnie oceniać. W wielu przypadkach szczegółowe ujawnianie danych na swój temat może wynikać z braku świadomości, że te dane są gromadzone i analizowane oraz wykorzystywane chociażby w marketingu, dzięki czemu można sterować naszymi wyborami konsumenckimi. Z drugiej strony ujawnianie tych informacji może być po prostu świadomym kosztem, który ponosimy za komfort ułatwiania nam różnego rodzaju wyborów, otrzymywania gotowych rozwiązań.

Coraz częściej można zaobserwować jednostkową manifestację prywatności i intymności. Zapewne jest to kwestia indywidualnych wyborów i wewnętrznych motywacji, ale – jak sadzę – również rosnących oczekiwań innych. Informacje o nas są gromadzone, nasza sfera prywatna staje się przedmiotem dyskursów, a ponadto nowe technologie skłaniają do odsłonięcia siebie, między innymi dlatego, że pozwalają na to w prosty i tani sposób. Ujawnienie swojej sfery prywatnej jest możliwe bez szczególnych predyspozycji i zasobów, bez wyodrębnionej, fizycznej przestrzeni, bez ograniczenia czasowego, bez uwikłania w relacje społeczne i relacje władzy. Odsłonięcie jest jednym z elementów życia i jako takie staje się naturalne, a następnie – oczekiwane. Odsłonięcie swojej prywatności występuje na tyle często, że staje się elementem codziennej interakcji nie tylko w gronie osób bliskich i zaufanych.

Informacje, które kiedyś zachowywaliśmy dla siebie, ewentualnie dzieliliśmy się nimi tylko w małym gronie, udostępniamy teraz szerokiemu audytorium. Zapewne w wielu przypadkach nie wiemy nawet, jak szerokiemu. Jeżeli bowiem zdaje się nam, że tych kilka intymnych, prywatnych spraw udostępnimy w grupie, którą definiujemy jako „znajomych”, to sieć, istniejąca bez granic czasowych i przestrzennych, może nas zaskoczyć. Współcześnie, dzięki nowym technologiom, przesyłanie informacji zajmuje przecież mniej niż kilka sekund. W wielu przypadkach sami odbieramy sobie prawo do tajemnicy, chociaż to prawo jest nam zagwarantowane przez regulacje prawne. Według *Webster Dictionary* słowem roku 2008 zostało *overshare*, oznaczające zbyt intensywne dzielenie się

informacjami na temat swojego życia prywatnego czy wręcz obarczanie nimi innych³².

W rzeczywistości aterytorialnej i beczasowej komunikacja staje się najważniejsza. Jak stwierdza Anna Młynarska-Sobaczewska: „Skoro zatem osiã, samym sensem i treścią tego świata jest komunikacja, pojęcie sfery wolnej od komunikacji, prywatności musi ulec przeobrażeniu wraz z całą tak zdiagnozowaną strukturą społeczną”³³.

Z jednej strony warto zwrócić uwagę na to, czy obowiązujące prawo chroni nas dostatecznie, a z drugiej strony – czy sami nie utrudniamy tej ochrony, która jest nam zapewniona. Dużym problemem jest zapewne to, że obecnie, dzięki dostępnym w każdej chwili urządzeniom rejestrującym, każdy nasz ruch może się stać obiektem internetowych dyskusji. Biorąc pod uwagę praktykę i już występujące zjawiska, na podstawie zarejestrowanego zdarzenia (czy może częściej – fragmentu zdarzenia) możemy się stać obiektem społecznego ataku. Wystarczy, że zarejestrowana sytuacja zostanie zinterpretowana lub celowo opisana w niekorzystny dla nas sposób. O ile jeszcze kilka lat temu publikowanie wizerunku obcych, przypadkowych osób nie było powszechne, o tyle obecnie może się zdarzyć, że zobaczymy swoje zdjęcie w Internecie, opatrzone dyskredytującym nas komentarzem. Internet stał się narzędziem interwencji społecznej, dlatego jeżeli nasze zachowanie zostanie zinterpretowane jako niezgodne z przyjętą normą lub normą, do której przestrzegania dana społeczność dąży, możemy się stać obiektem osądu lub celem ataku. Coraz trudniej jest zatem orzekać, które dziedziny życia i aktywności pozostają (czy powinny pozostać) w sferze prywatności, tajemnicy i autonomii informacyjnej – a tym samym podlegać ochronie.

To, co dawniej pozostawało w sferze prywatnej, dzisiaj (czasem bez względu na to, czy tego chcemy, czy nie) przenika – lub przynajmniej istnieje zagrożenie, że przeniknie – do sfery jawnej,

³² A. Młynarska-Sobaczewska, *Trzy wymiary...*, s. 42.

³³ *Ibidem*, s. 45.

dostępnej dla wszystkich innych użytkowników nowych mediów. Nawet pobieżne badanie treści portali internetowych pozwala na wychwycenie przypadków upublicznienia informacji, często intymnych, wbrew woli ich nadawcy lub adresata. Ponadto trudno obecnie mówić o właściwych i adekwatnych do sytuacji regulacjach prawnych, które zapewniałyby ochronę prywatności.

Przenikanie się sfer prywatnej i publicznej powoduje, że coraz trudniej określić granicę, która oddziela te dwie sfery. Oprócz sfery prywatnej przeobrażeniu uległa bowiem także sfera publiczna. „Publiczne” oznacza to, co jawne, dostępne dla innych. Jest przeciwieństwem tego, co prywatne – tajne, ukryte. Według Wiesława Hładkiewicza zmiany w zakresie tego, co publiczne były uzależnione od tego, co i na jakiej zasadzie było ujawniane, a także komu było ujawniane oraz na jaką skalę³⁴.

Jak już wspomniałam, w świecie antycznym przestrzeń publiczną kojarzono z wolnością, z trwaniem, i była ona całkowicie odseparowana od aktywności domowych, tych służących jedynie podtrzymaniu życia. W średniowieczu, według Jürgena Habermasa, mieliśmy do czynienia z reprezentacyjną sferą publiczną, która nie miała charakteru komunikacyjnego, ale raczej oznaczała demonstrowanie swojego statusu społecznego. Rozwój kapitalizmu i nowoczesnych społeczeństw skutkowało wykształceniem się mieszczańsko-obywatelskiej sfery publicznej. Kształtujące się społeczeństwo obywatelskie zażądało transparentności i jawności władzy³⁵.

Rozwój prasy oraz tworzenie klubów i miejsc publicznej dyskusji przyczyniły się do powstania mieszczańskiej sfery publicznej. Współcześnie, według Habermasa, społeczeństwo masowe i komercjalizacja mediów przyczyniają się do zawężenia sfery publicznej³⁶.

³⁴ W. Hładkiewicz, *Koncepcja przestrzeni publicznej w teorii krytycznej Jürgena Habermasa*, w: *Sfera publiczna. Kondycja – przejawy – przemiany*, red. J.P. Hudzik, W. Woźniak, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2006, s. 143.

³⁵ K. Jaskułowski, *Koncepcja sfery publicznej Jürgena Habermasa*, „Spotkania Europejskie” 2010, nr 3, s. 73–75.

³⁶ A. Elliott, *Współczesna teoria społeczna*, przeł. P. Tomanek, Wydawnictwo Naukowe PWN, Warszawa 2011, s. 190–191.

Prasa wydawana na masową skalę umożliwiła rzeczywiście szeroki dostęp do informacji i sfery publicznej, ale komercyjne nastawienie sprawia, że sfera publiczna staje się odpolityczniona. Habermas przywołuje przykład prasy groszowej, w której, w zamian za większą sprzedaż, rezygnowano z treści politycznych, „eliminując wiadomości polityczne i polityczne artykuły wstępne na rzecz takich moralnych zagadnień jak nieumiarkowanie i hazard”³⁷.

W opinii Habermasa rzeczywistość wykreowana przez media masowe tylko na pozór stanowi sferę publiczną. Współczesne media stały się bowiem miejscem publikowania prywatności i miejscem dla reklamy. Im większe znaczenie ma sfera publiczna jako środek wpływu politycznego i ekonomicznego, tym bardziej staje się apolityczna. W modelu obywatelskiej sfery publicznej podział na życie prywatne i publiczne był klarowny. Na sferę publiczną składali się indywidualni obywatele, którzy stanowili publiczność pośredniczącą między państwem a potrzebą społeczną. Przenikanie się obszarów skutkowało powstaniem upolitycznionej sfery społecznej, której nie można zaliczyć ani do sfery prywatnej, ani do sfery publicznej³⁸.

Według Richarda Sennetta współczesność możemy porównywać z okresem upadku Cesarstwa Rzymskiego. Punktem stycznym byłby tutaj kryzys równowagi między sferami publiczną i prywatną. Rzymianie schyłku epoki augustiańskiej traktowali sferę publiczną jedynie jako obszar formalnych zobowiązań, rytuałów i ceremonii. Ich zaangażowanie w sprawy polityczne malało. Zwrócili się w stronę sfery prywatnej, w której szukali ucieczki od świata. Sennett zauważa, że dzisiejsze życie publiczne również jest sformalizowane, a uczestnictwo w nim sprowadza się do podporządkowania władzy i przyzwolenia. Naszą współczesność od czasów rzymskich różni podejście do sfery prywatnej: „Rzymianin poszukiwał w sferze prywatnej zasady, którą mógłby przeciwstawić sferze publicznej –

³⁷ J. Habermas, *Strukturalne przeobrażenia sfery publicznej*, przeł. W. Lipnik, M. Łukasiewicz, Wydawnictwo Naukowe PWN, Warszawa 2007, s. 319–320.

³⁸ *Ibidem*, s. 330–334.

zasady opartej na religijnej transcendencji świata. My nie szukamy zasady, ale refleksji, zrozumienia tego, czym jest nasza psyché, co jest autentyczne w naszych uczuciach. Z przebywania w prywatności, wyłącznie w towarzystwie własnym oraz rodziny i bliskich przyjaciół próbujemy uczynić cel sam w sobie³⁹.

Wiele wskazuje na to, że obecnie mamy do czynienia ze schyłkiem sfery publicznej. Na pewno ma ona inny kształt niż ten znany światu antycznemu. Dla Zygmunta Baumana wyłonienie się współczesnego społeczeństwa oznaczało zwycięstwo prywatności, ale także wieściło jej zmierzch. Prywatność „skolonizowała sferę publiczną”, ale jednocześnie utraciła swoje bardzo ważne przywileje – tajemnicę i dyskrecję⁴⁰.

Obywatel i państwo

Debata dotycząca relacji między zapewnieniem bezpieczeństwa a ochroną danych obywateli rozgorzała w 2005 roku, po ujawnieniu przez gazetę „New York Times” informacji o inwigilacji obywateli Stanów Zjednoczonych. Po ataku terrorystycznym z 11 września 2001 roku prezydent George W. Bush zezwolił Narodowej Agencji Bezpieczeństwa (National Security Agency, NSA) na korzystanie z wielu programów podsłuchowych i inwigilacji elektronicznej. Po 2001 roku powstało około czterdziestu centrów informacji, które gromadzą dane z zakresu między innymi bankowości, finansów, rynku nieruchomości, edukacji czy turystyki. W 2006 roku w mediach pojawiła się informacja o tym, że NSA zbiera szczegółowe dane telekomunikacyjne. W sektorze prywatnym korporacje gromadzą dane, także te wrażliwe, obejmujące między innymi informacje dotyczące demografii, wyznania, wielko-

³⁹ R. Sennett, *Upadek człowieka publicznego*, przeł. H. Jankowska, Warszawskie Wydawnictwo Literackie Muza SA, Warszawa 2009, s. 11–13.

⁴⁰ Zob. Z. Bauman, D. Lyon, *Płynna inwigilacja...*, s. 46.

ści majątku, przeprowadzanych operacji finansowych czy numery rejestracyjne pojazdów⁴¹.

Problematyka ingerowania państwa w autonomię informacyjną, czyli w nasze prawo do tajemnicy, jest bardzo złożona⁴². Według niektórych szacunków liczba informacji gromadzonych o obywatelach z roku na rok podwaja się, zdolność do ich przetwarzania wzrasta w postępie geometrycznym, a samo przetwarzanie staje się coraz tańsze⁴³.

Potencjalnym zagrożeniem jest również możliwość powstawania regulacji, które ograniczają swobody obywatelskie w imię zapewnienia bezpieczeństwa. Ten konflikt będzie wyrażany w konfrontacji między dobrem ogółu i dobrem jednostki. To dylemat, który nastęrcza wielu trudności, także tych definicyjnych i normatywnych. Interes publiczny jest kategorią normatywną. Wartości podstawowe i wspólne dla społeczności – na przykład ochrona zdrowia – są bezsprzecznie składową interesu publicznego, nie sposób jednak na drodze prawnej precyzyjnie określić, czym jest dobro ogółu wpisane w cele działania państwa. Dlatego decyzyjność w tej kwestii ma również administracja, a określenie, czym jest interes publiczny może być także przejawem woli politycznej.

W sytuacji powszechnego gromadzenia informacji o nas problem ich wykorzystywania, także przez państwo, nabiera głębokiego znaczenia. Posługując się terminem, który wprowadził Gilles Deleuze: żyjemy w „społeczeństwach kontroli” (*society of control*)⁴⁴,

⁴¹ B. Mucha, *Data mining a współczesny kształt prawa do prywatności w Stanach Zjednoczonych*, w: *Bezpieczeństwo państwa...*, s. 135–144.

⁴² Na poziomie normatywnym warto przywołać klasyczne sformułowanie zawarte art. 8 ust. 2 *Europejskiej konwencji praw człowieka*: „Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób”. *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r.*, „Dziennik Ustaw” 1993, nr 61, poz. 284.

⁴³ B. Mucha, *Data mining...*, s. 136.

⁴⁴ G. Deleuze, *Postscriptum o społeczeństwach kontroli*, w: *idem, Negocjacje 1972–1990*, tłum. M. Herer, Wydawnictwo Naukowe Dolnośląskiej Szkoły Wyższej, Wrocław 2007.

czyli w społeczeństwach, w których inwigilacja nie rozrasta się wertykalnie i w uporządkowany sposób, ale rozprzestrzenia się jak chwasty⁴⁵. Według Zygmunta Baumana współczesny świat jest postpanoptyczny – kontrola nie wymaga już obecności nadzorców. Ponadto kontrola nie kojarzy się już z więzieniem. Wręcz przeciwnie – narzędziami kontroli mogą być te same przedmioty, które wykorzystujemy do zabawy i rozrywki. Nasze telefony komórkowe i komputery są wielkimi bazami danych o nas samych.

Coraz częściej zgadzamy się na to, żeby informacje o nas były gromadzone i przetwarzane. Tym samym decydujemy o tym, że rezygnujemy z tajemnicy. Życie w społeczeństwie ryzyka (*risk society*) – posługując się terminem ukutym przez Ulricha Becka⁴⁶ – skłania do tego, żeby rezygnować z części swojej prywatności za cenę poczucia bezpieczeństwa. Nie bez podstawy coraz popularniejszy staje się termin „rynek strachu”. Źródeł zagrożeń jest coraz więcej, a ich oblicza zmieniają się szybciej niż kiedykolwiek wcześniej. Systemy zabezpieczeń, oprócz tego, że mają nas chronić, wzmagają ten strach. Jeżeli jesteśmy monitorowani na coraz większą skalę, obcujemy z coraz większą liczbą urządzeń, zabezpieczeń i coraz częściej jesteśmy poddawani kontroli, to poczucie zagrożenia rośnie wraz ze wzrostem zakresu inwigilacji.

Podsumowanie

Rozwój społeczeństwa wraz z rozwojem technologicznym i ewolucją w stronę społeczeństwa informacyjnego zmienia oblicze tajemnicy. Nakłada zupełnie nowe obowiązki na państwo i prowadzi do powstania nowych zagrożeń dla bezpieczeństwa. W perspektywie jednostkowej wpływa na postrzeganie przez nas prywatności. Zmienia naszą perspektywę tego, co publiczne, przekształca sferę

⁴⁵ Z. Bauman, D. Lyon, *Płynna inwigilacja...*, s. 12.

⁴⁶ U. Beck, *Społeczeństwo ryzyka. W drodze do innej rzeczywistości*, tłum. S. Cieśla, Wydawnictwo Naukowe Scholar, Warszawa 2004.

publiczną czy – zgodnie z wieloma głosami – doprowadza do schyłku sfery publicznej, w zamian oferując jej pozór.

Dotychczasowe regulacje prawne dotyczące ochrony informacji dezaktualizują się, a przynajmniej zaczynają być niewystarczające. Być może tajemnica, którą tak wysoko ocenił wspomniany na początku Georg Simmel, w perspektywie jednostkowej nie jest już tak pociągająca. Może rację miał Zygmunt Bauman, kiedy stwierdzał, że dziś bardziej niż odkrycia naszych sekretów i intymności boimy się, że zostaniemy zamknięci w naszej sferze prywatnej. Bardziej obawiamy się tego, że nie będziemy mieli sposobności i audytorów, przed którymi będziemy mogli się ujawnić. Z drugiej strony współczesne państwa mają coraz większe potrzeby informacyjne i, co bardzo prawdopodobne – coraz większą potrzebę tajności. Podobnie jak organizacje, korporacje i wielkie instytucje. A my sami te potrzeby informacyjne – świadomie lub nieświadomie – zaspokajamy.

Secrecy and openness in the context of information protection

The goal of this article is to present the issues of secrecy and transparency in the context of information security and autonomy of information in the information society. It describes the role of information and its significance in the functioning of the state, as well as needs and threats in the field of information security. The second part of the article discusses aspects of citizens' rights to secrecy, protection of privacy and sensitive data. It also characterises changes in the concept of autonomy of information, the public sphere and the private sphere. The third part discusses the issue of relations between state and citizen in the context of collection, storage and use of information.

Keywords: secrecy, openness, citizens, privacy rights, data protection.