*Marie-Therese Tinnefeld*

# Jak Internet zmienia prawne ramy prywatności?

## 1. Wstęp

Rozwój kształtuje swoje własne obrazy. Dotyczy to również prawa do prywatności i jego prawno-kulturowej interpretacji w Internecie. Tam, gdzie podejmowane są decyzje za albo przeciw prywatności człowieka, tam mamy do czynienia z obrazami człowieka. Różnie są one odbierane – historycznie lub współcześnie, na wzór zachodni lub wschodni, realnie lub wirtualnie. Koncepcja obrazu człowieka zawiera w sobie pytanie, jaką wartość nadamy człowiekowi i jego prywatności, od jakich przesłanek jest ona zależna, co jest jej właściwą funkcją, dlaczego zakłada się, że **prywatność** jest istotną „przesłanką obszarów wolności w rozumieniu praw człowieka"[1].

Temat obrazu człowieka cieszy się szczególną popularnością każdorazowo w czasach zrywów i przekształceń, kryzysów i przełomów, niepewności i poszukiwania sensu powodowanych postępem, roszczeń wolnościowych i żądań bezpieczeństwa. Tak było w czasach Oświecenia, na przełomie XVII i XVIII w., kiedy ludzie z podwładnych stali się obywatelami. Konfrontacja z „faszystowskimi" i „socjalistycznymi" obrazami człowieka przenika historię Europy XX w. Dopiero wraz z przełomem politycznym pod koniec ubiegłego wieku oraz upadkiem tzw. Żelaznej Kurtyny (1989 r.) ludzie ze Wschodu i Zachodu Europy odnaleźli się wspólnie jako równouprawnieni obywatele w otwartych systemach demokratycznych, z prawem do niekontrolowanej prywatności, bez szpiegowania ich przestrzeni prywatnych. W dzisiejszym procesie **rewolucji cyfrowej** ludzie, z pomocą subtelnych technologii informacyjnych i komunikacyjnych, wkraczają w wirtualne przestrzenie wraz z ich licznymi sieciami społecznościowymi, w których za pomocą słów i obrazów

[1] *M.-T. Tinnefeld*, Privatheit als Voraussetzung menschenrechtlicher Freiräume?, Datenschutz und Datensicherheit (DuD) 2011, t. 35, Nr 9, s. 598–601.

udzielają informacji prywatnych i intymnych. A zatem – czyżby erozja prywatności?

Pytanie o prywatność zawsze wiąże się z udaną, funkcjonującą demokracją[2]. W epoce wszechobecnej komunikacji życie demokratyczne zmienia się: publiczność błyskawicznie jest informowana przez polityków, blogerów i dziennikarzy o wyborach czy o politycznych przełomach (np. na Bliskim Wschodzie), często jednak brakuje krytycznego przetwarzania informacji, a także właściwej ochrony prywatności osób, których informacja dotyczy – ochrony choćby przed informatorami. Interesującym tego przykładem są działania dochodzeniowe dokonywane przez WikiLeaks[3].

Ponadto platformy takie jak YouTube lub Facebook otwierają zorganizowanej przestępczości bezpośredni dostęp do milionów użytkowników, którzy ochoczo udostępniają tam, w słowach i obrazach, informacje o sobie[4]. Procesy wyszukiwania w Internecie dokonują się w sposób niewidoczny i spersonalizowany. Spersonalizowane filtry stosowane są przez gigantów Internetu, takich jak Google, Facebook, Apple i Microsoft, w myśl zasady: „You're are getting a free service, and the cost is information about you"[5]. Czyżby zatem pieniądze zamiast wolności?

Filtry i sieci wyszukiwania wykorzystywane są również – w interesie bezpieczeństwa wewnętrznego i zewnętrznego – przez państwowe organy bezpieczeństwa w celu poszukiwania potencjalnych przestępców, terrorystów, pedofilów czy niebezpiecznych hackerów[6]. Warto przywołać choćby kontrowersyjną metodę zatrzymywania danych, która wraz z dyrektywą 2006/24/WE przyniesie masowe ograniczenia wolności[7]. A zatem – bezpieczeństwo kontra wolność?

Istnieją jeszcze specyficzne punkty styczne między prawem a „kulturą obywatelską" tj. kulturą zbudowaną na prawach człowieka. Znajdują się one w deklaracji praw człowieka – Declaration of Human Rights – z 1948 r. i w następujących po nich deklaracjach praw człowieka i praw podstawowych. Niżej zostaną ukazane poszczególne obszary ochrony prywatności w kontek-

[2] Tak orzekł już Federalny Trybunał Konstytucyjny (*Bundesverfassungsgericht*, BVerfGE) w swoim przełomowym wyroku dotyczącym ewidencji ludności – BVerfGE 65, 1.

[3] *M. Rosenbach*, *H. Stark*, Staatsfeind WikiLeaks, Wie eine Gruppe von Netzaktivisten die mächtigsten Nationen der Welt herausfordert (Deutsche Verlags-Anstalt 2011).

[4] W związku z wyzwaniami przy zwalczaniu przestępczości internetowej, por. *M. Gercke*, *Ph. W. Brunst*, Praxishandbuch des Internetstrafrechts (Kohlhammer W. 2009), s. 7–39.

[5] *E. Pariser*, The Filter Bubble. What the Internet Is Hiding from You (Penguin Press 2011), s. 6f.

[6] W związku z tym pojęciem zob. *S. Gaycken*, Caberwar, Das Internet als Kriegschauplatz (Open Source Press 2011), s. 25–58.

[7] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15.3.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.Urz. UE L 105 z 13.4.2006 r., s. 54).

ście Europejskiej Konwencji Praw Człowieka (art. 8 EKPC), Karty Praw Podstawowych Unii Europejskiej (art. 7 i 8 EKPP) oraz krajowych konstytucji opartych na prawach człowieka (por. np. art. 2 ust. 1 w zw. z art. 1 ust. 1 Ustawy Zasadniczej RFN) oraz zostaną przestawione możliwości ich zastosowania w świecie sieci.

## 2. Ochrona prywatności na gruncie praw podstawowych

Wyrok niemieckiego Federalnego Trybunału Konstytucyjnego (FTK) w sprawie spisu ludności[8] postrzegany jest jako kamień milowy w historii ochrony prywatności. Z zakorzenionego w katalogu praw podstawowych niemieckiej Ustawy Zasadniczej ogólnego prawa do ochrony i rozwoju własnej osobowości Trybunał – w warunkach automatycznego przetwarzania danych w 1983 r. – wywiódł prawo podstawowe do ochrony danych osobowych (art. 2 ust. 1 – ogólne prawo do rozwoju własnej osobowości, i art. 1 ust. 1 Ustawy Zasadniczej RFN – poważanie godności ludzkiej). Trybunał połączył owo „nowe" prawo z prawem do prywatności, tak jak opisali to już *Alan Westin* oraz *Samuel D. Warren* i *Louis Brandeis*[9].

Zasady ochrony danych osobowych są istotne również w kontekście szczególnych praw podstawowych, np. w związku z przetwarzaniem danych pozyskanych z podsłuchu w mieszkaniu lub z podsłuchu środków telekomunikacji. Prawo podstawowe do ochrony w związku z technologiami informacyjnymi, również wywiedzione przez Trybunał – w 2008 r. – z ogólnego prawa do ochrony i rozwoju własnej osobowości, stanowi kolejny duży krok w rozwoju ochrony prywatności na gruncie praw podstawowych wobec kontroli ze strony państwa. Prawo to chroni własny system informatyczny użytkownika przed potajemną ingerencją państwa i osób trzecich. Szczególny zakres jego uregulowania nie może być w tym opracowaniu omówiony w sposób pogłębiony.

### 2.1. Ochrona danych osobowych (art. 8 EKPC, art. 8 EKPP, art. 2 ust. w zw. z art. 1 ust. 1 Ustawy Zasadniczej RFN)

Ochrona danych osobowych tudzież prawo do samodzielnego rozporządzania informacjami o sobie mają na celu zagwarantowanie ochrony wolności człowieka przed informacyjną dominacją państwa lub podmiotów trzecich, w szczególności podmiotów gospodarczych. Margines wolności na rzecz jednostki konieczny jest szczególnie wtedy, gdy jednostka opuszcza swoją sferę przestrzennej wolności w ścisłym znaczeniu i nawiązuje relacje z otoczeniem. „Społeczna ochrona sfery prywatnej skierowana jest przede

[8] BVerfGE 65, 1.

[9] *A. Westin*, Privacy and Freedom (Atheneum, New York 1967); *S. D. Warren, L. D. Brandeis*, The Right to Privacy, Harvard Law Review 1890, t. 4, Nr 5, s. 193 i n.

wszystkim przeciwko zbyt precyzyjnym oczekiwaniom innych co do identyfikowalności"[10]. Prawo to ma gwarantować jednostce – dodatkowo do danej jej możliwości wycofania się w prywatność swego mieszkania – również w kontaktach z otoczeniem mentalne (wewnętrzne) przestrzenie życia prywatnego. Z tego względu prawo ochrony danych osobowych wytworzyło określone zasady[11]:

1. Zasada związku z celem: wiąże ona administratora danych i pozwala mu na przetwarzanie wyłącznie tych danych, które niezbędne są do realizacji danego celu.
2. Tak zwany trójgłos w kwestii dopuszczalności: składa się on ze świadomej, tj. udzielonej po otrzymaniu informacji, zgody jako zasady dopuszczalności lub z ogólnych i szczegółowych regulacji ustawowych.
3. Wymóg transparentności: oznacza otwartość i przejrzystość działań gospodarczych podmiotów publicznych i prywatnych.
4. Poszukiwanie możliwej alternatywy dla ingerencji w prywatność: tu w rachubę wchodzą między innymi formy „ascezy danych" poprzez przetwarzanie danych anonimowo lub pod pseudonimem, a także przez ochronę danych osobowych przy zastosowaniu techniki.
5. Bezwzględna ochrona rdzennego obszaru życia prywatnego.
6. Możliwość kontroli przez obywateli (prawo do informacji i powiadomień) oraz korekty (prawo do kasowania, korekty danych oraz zamykania dostępu do danych).
7. Kontrola przez niezależne instancje powołane do ochrony danych.

Podporządkowanie zasadom i kontrola stanowią normatywne środki, którymi ustawodawca chce przywiązać potężnych administratorów danych do ich ochrony. Nie chodzi przy tym wyłącznie o szanse swobodnego rozwoju jednostki, ale także o demokrację i jej warunek: świadomego, doinformowanego obywatela (*citoyen*) – wolnego od manipulacji i zastraszania przez państwa lub podmioty trzecie. W świecie sieci należą do nich w szczególności operatorzy Facebooka, Twittera, Google i innych.

## 2.2. Prywatność w rozumieniu przestrzennym (art. 8 EKPC, art. 7 EKPP, art. 13 Ustawy Zasadniczej RFN)

Do swobodnego rozwoju człowiekowi niezbędne są przestrzenie, w których może on się realizować, w których może przeżywać i wyrażać swoje uczucia i myśli w sposób nieskrępowany i nieobserwowany, wspólnie

[10] *B. Rössler*, Der Wert des Privaten (Suhrkamp Verlag, Frankfurt am Main 2001), s. 209.

[11] Zob. *M-T. Tinnefeld* i in., Einführung in das Datenschutzrecht (Oldenbourg Wissenschaftsverlag; 5. wydanie w trakcie publikacji).

z innymi, z którymi łączą go przyjazne stosunki[12]. Podsłuchiwanie mieszkań jest ważnym przykładem na to, jak niewiele pozostaje z prawa podstawowego do mieszkania, tj. do prywatności w rozumieniu przestrzennym, skoro nawet niepodejrzewane osoby kontaktowe mogą być potajemnie podsłuchiwane, a wszystkie dane rejestrowane. Tego typu ingerencji nie usprawiedliwia nawet międzynarodowy terroryzm. W swym orzeczeniu dotyczącym tzw. dużego ataku podsłuchowego[13] FTK pokreślił, że ludzie muszą móc ufać w to, że najbardziej osobista, wewnętrzna sfera prywatności będzie podlegała ochronie. Rdzeń prywatności, życie intymne, musi pozostać nienaruszone. Ta sfera musi – nawet wobec bardzo poważnych względów bezpieczeństwa czy względów gospodarczych – pozostać poza obserwacją, w tym zakresie zachowana została „kultura obywatelska". W podobny sposób wyraża się czeski pisarz *Milan Kundera*, który wobec tendencji do upubliczniania życia i umierania ludzkiego stwierdza, że „jeżeli stanie się nawykiem i regułą, że czyjąś intymność przenosi się do ogólnej sfery międzyludzkiej, to wkraczamy w epokę, w której ważą się losy przeżycia lub zaniku indywidualnej jednostki"[14].

Niepokoi zatem fakt, że wiele osób dobrowolnie, za pośrednictwem kamery, wstawia do Internetu prywatne lub intymne dane i zdjęcia z własnych mieszkań. Jeszcze więcej zastrzeżeń budzi sytuacja, gdy ludzie upubliczniają w sieci zdjęcia innych osób, np. zdjęcia z grilla w ogrodzie u sąsiada. W ten sposób rezygnuje się z koniecznych form bliskości i dystansu, przez które to formy społeczne relacje nabierają dopiero swego swoistego znaczenia[15].

Zastanawiające jest również wyrażanie zgody przez obywateli korzystających z sieci dla celów komunikacji elektronicznej. Wraz z przyjęciem się modelu Web 2.0 Internet stopniowo stał się medium dwutorowym. Rozprzestrzenienie się takich platform jak YouTube czy Facebook skłania wiele osób do upubliczniania swoich danych osobowych. Inspektorzy ochrony danych wzywają np. użytkowników do usuwania *fan page* z Facebooka, tzw. S*ocial--Plugins*, czy przycisku „Lubię to" ze swych stron internetowych, ponieważ przekazywane w ten sposób dane są spersonalizowane i mogą być wykorzystywane do innych celów, niezgodnych z ochroną danych osobowych[16]. Są

[12] *Ch. Hohmann-Dennhardt*, Freiräume – Zum Schutz der Privatheit, [w:] *G. Duttge, M.-T. Tinnefeld* (red.), Gärten, Parkanlagen und Kommunikation. Lebenräume zwischen Privatsphäre und Öffentlichkeit (Berliner Wissenschafts-Verlag 2006), s. 85 i n.

[13] BVerfGE 109, 361; zum Kerngehalt privater Lebensgestaltung s.a BVerfGE 120, 180.

[14] *M. Kundera*, Zdradzone testamenty, przeł. *S. Roth*, Hanser 1994, s. 248.

[15] Zob. G. Simmel, Soziologie. Untersuchungen über Formen der Vergesellschaftung. Gesamtausgabe Bd. II, herausgegeben von O. Ramstedt (Suhrkamp Verlag, Frankfurt a.M. 1992), s. 391, 397.

[16] Zob. https://www.datenschutzzentrum.de/presse/20110819-facebook.htm: „Przy korzystaniu z funkcjonalności Facebooka dochodzi do przekazania danych dotyczących ruchu oraz

to nowe wyzwania, z którymi muszą się zmierzyć państwa, gospodarki oraz społeczeństwa[17].

### 2.3. Poufna komunikacja (art. 8 EKPC, art. 10 Ustawy Zasadniczej RFN)

Ochronie komunikacji poufnej podlegają konwencjonalne (np. poczta), ale również nowoczesne formy komunikacji (np. e-mail, SMS). Ochrona komunikacji (odbywanej poprzez pośredników) obejmuje treść komunikacji oraz okoliczności komunikacji z udziałem osób trzecich, tj. również dane dotyczące połączeń. Zakres tej ochrony odgrywa centralną rolę w debacie o zatrzymywaniu danych. Unia Europejska uważa dyrektywę 2006/24/WE za „wartościowy instrument dla systemów wymiaru sprawiedliwości i organów ścigania w UE"[18]. Nawet jeśli zatrzymywanie przez usługodawców telekomunikacyjnych informacji dotyczących przepływu danych miałoby być przydatne dla organów bezpieczeństwa i organów ścigania przy wykonywaniu ich statutowych zadań, wątpliwe jest, by czyniło ono zadość panującej w ochronie danych osobowych zasadzie konieczności i współmierności[19].

Kolejny dylemat wynika z faktu, że ustawodawca przy wykonywaniu swoich słusznych zadań nie zawsze w sposób wystarczający bada skutki i następstwa konkretnego zastosowania technicznego, np. w walce ze straszliwą pornografią dziecięcą. Blokady dostępu do Internetu są pod wieloma względami kontrproduktywne: listy zamkniętych adresów mogą być odtwarzane przy zastosowaniu specjalnych strategii wyszukiwania i mogą stanowić swoiste „zalecenia" dla zainteresowanych kryminalistów. Natomiast zasada „kasować zamiast blokować" wolna jest od szkodliwych efektów ubocznych i może być stosowana na całym świecie. W żadnym bowiem kraju świata, w którym udostępniane są serwery, producenci i dystrybutorzy pornografii dziecięcej nie podlegają ochronie. Z tego powodu możliwe jest szybkie transgraniczne kasowanie treści na serwerach. Dodatkowo należy uwzględnić okoliczność, że wykształcona infrastruktura blokująca może zostać wykorzystana do cenzuro-

treści do USA oraz do zwrotnego kwalifikowanego komunikatu do użytkownika, tzw. analiza zasięgu. Ktokolwiek kiedykolwiek korzystał z Facebooka lub z wtyczki internetowej może wychodzić z założenia, że przez dwa lata namierzany («trakowany») jest przez to przedsiębiorstwo. W Facebooku sporządzany jest profil osoby, w przypadku członków nawet spersonalizowany".

[17] Zob. dokument Rady Inernetowej CSU „In Freiheit und Fairness" pod adresem: http://www/csu.de/dateien/partei/dokumente/11031_positionspapier_netzrat.pdf.

[18] Raport z 18.4.2011 – KOM(2011) 225 final, s. 1.

[19] W związku z uzasadnionymi wątpliwościami w świetle ochrony praw podstawowych, por. Thomas Petri, Dyrektywa 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych telekomunikacyjnych, DuD 2011, Nr 9, s. 607–610.

wania innych treści i w związku z tym może stanowić zagrożenie dla wolności słowa i dostępu do informacji[20].

### 2.4. Przywilej mediów

Ochrona danych osobowych i wolność dostępu do informacji są wzajemnie od siebie zależne. Obydwa te prawa umożliwiają dopiero korzystanie z demokratycznych swobód[21]. Jednostka zdana jest na obszerny dostęp do informacji, jeżeli ma mieć szansę wykształcenia w sobie opinii na jakiś temat. W ramach EKPC oraz EKPP prawo dostępu do informacji postrzegane jest głównie jako element wolności opinii (art. 10 EKPC, art. 10 EKPP, art. 5 ust. 1 zd. 2 Ustawy Zasadniczej RFN). Jej istotą jest zagwarantowanie obywatelom dostępu do informacji, co stanowi antidotum na „podstawowe zło" w działaniu państwa, mianowicie działanie potajemne.

Funkcjonalne znaczenie wolności opinii oraz wolności prasy jest niemożliwe do przecenienia. Zasadne jest jednak również pytanie o granice, które zbieraniu i publikowaniu informacji prywatnych i poufnych wyznacza ochrona prywatności[22]. Dyrektywa UE o ochronie danych osobowych[23] udziela wprawdzie mediom przywileju. Przywilej ten jest jednak istotnie ograniczony z uwagi na ochronę danych osobowych[24].

Potężna platforma internetowa WikiLeaks jest uosobieniem koncepcji ogólnoświatowej społeczności połączonej siecią, wedle której to koncepcji każda informacja musi być swobodnie dostępna, i to użytkownik ma mieć kontrolę nad tym, jakie informacje chce przywołać. Na pierwszy rzut oka wygląda to na niezakłócone zaufanie do korzystających z sieci obywateli i mogłoby stanowić zaawansowany model demokracji, przy bliższym spojrzeniu nabiera jednak innego wymiaru. W większości brakuje jakichkolwiek widocznych samoograniczeń przy publikacji zdobytych w hakerski sposób informacji, które to ograniczenia właściwe są dla wysokiej jakości dziennikarstwa. Publikowanie na całym świecie amerykańskich depesz bez względu na dany kontekst kulturowy, bez względu na ochronę prywatności informatorów i dyplomatów, narusza ich dobra osobiste. Inna ocena byłaby zasadna tylko wtedy, gdyby upubliczniane

[20] Do kwestii „Znaków Stop" w Internecie zob. *M.-T. Tinnefeld*, Stopp-Schilder in Internet, DuD 2010, t. 34, Nr 1, s. 15–19.

[21] Tak już BVerfGE 65, 1 – wyrok w sprawie ewidencji ludności, utrwalone orzecznictwo.

[22] *J. Abr. Frowein*, [w:] Frowein/Peukert, Komentarz do EKPC (Engel Verlag 2009, wyd. 3), s. 399.

[23] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. WE L 281 z 23.11.1995 r., s. 31, ze zm.).

[24] Por. art. 9 dyrektywy 95/46/WE, który stanowi, że przetwarzanie danych „wyłącznie dla celów dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego" dopuszczalne jest wtedy, gdy okaże się konieczne dla wyważenia ochrony prywatności ze swobodą mediów.

były poważne patologie lub poważne występki danych osób[25]. Innymi słowy, każdy człowiek potrzebuje chronionych przestrzeni komunikacji, jeżeli ma być zdolny do wolnego, również w rozumieniu politycznym, działania. Należy domniemywać, że obszar arkanów polityki będzie się znowu zwiększać, a tajna dyplomacja znów przybierać na znaczeniu[26].

## 3. Uwagi końcowe

Internet umożliwia wprawdzie ludziom, państwom, gospodarkom oraz mediom szybsze i bardziej elastyczne reagowanie na wydarzenia w przestrzeni rzeczywistej. Jednocześnie ogólnoświatowa sieciowa komunikacja i przetwarzanie danych powodują powstanie nowych zagadnień z punktu widzenia ochrony praw podstawowych, które zostały wyżej pokrótce nakreślone: ochrona prywatności i swobody dostępu do informacji w otwartych sieciach oraz zabezpieczenie wielorodności kulturowego sposobu postrzegania problemów.

Szczególny problem z punktu widzenia ochrony praw podstawowych stanowi fakt, że obywatele często nie są świadomi wartości swojej prywatności i nie tylko otwierają dostęp do swoich najbardziej osobistych danych – zwłaszcza w portalach społecznościowych – lecz także udostępniają je nieodpłatnym serwisom. Taka postawa prowadzi do tego, że również państwa, w interesie bezpieczeństwa, mogą sięgać do coraz większej liczby danych osobowych i nie natrafiają przy tym na istotny opór tych, których to dotyczy. Bez wątpienia ustawodawcą – tym narodowym, jak i tym ponadnarodowym – kierują w zakresie polityki bezpieczeństwa bardzo ważne cele. Jeżeli jednak Unia Europejska w celu zwalczania terroryzmu i cyberprzestępczości ogranicza zakres swobód obywatelskich, to z całą stanowczością należy zadać pytanie o jednoznaczne ukierunkowanie na ochronę praw podstawowych. Tu pojawia się kolejny problem, że już rzekome, tylko ponoszone (a jeszcze niepotwierdzone) zagrożenie wyłącza (daną kwestię) spod publicznej oceny i przenosi (ją) w „arkana", które od zawsze były „obszarami wolnymi od argumentacji"[27]. Dodatkowo dochodzi fakt, że prawa i swobody obywatelskie nie są właściwie wyważone, bo skutki i następstwa danego zastosowania technicznego (np. blokad dostępu do Internetu) są niedostatecznie dobrze znane.

Rewolucja cyfrowa każe postrzegać wiele spraw bliskich i dobrze znanych w innym świetle. Przy wszystkich próbach interpretacji i tłumaczenia nie można jednak pomijać faktu, że życie człowieka i jego kształtowanie zawsze

[25] Por. depesza z 31.7.2009 r. w WikiLeaks: Cable Viewer pod adresem: http://wikileaks.org/cablegate.html.

[26] *Ch. Möllers*, Zur Dialektik der Aufklärung der Politik, [w:] WikiLeaks und die Folgen (Suhkamp 2011), s. 195 i n.; tamże, *W. Ischinger*, Das WikiLeaks Paradox: Weniger Transparenz, mehr Geheimdiplamtie, s. 155 i n.

[27] *G. Baum*, Rettet die Grundrechte (Kiepenheuer & Witsch Verlag 2009), s. 27 i n.

związane jest z danym obszarem geograficznym i kulturowym, które nie są anulowane przez przestrzeń wirtualną, na które jednak ta przestrzeń wirtualna w istotny sposób oddziałuje. Ochrona danych osobowych w cyfrowym świecie powinna zatem bazować na sprawdzonych zasadach i środkach kontroli, aczkolwiek w odpowiednio zmodyfikowanej formie. Ochrona danych osobowych powinna niejako zostać „wbudowana" tudzież „zintegrowana" w technologie sieciowe.

## Podsumowanie

Pojęcie prywatności i ograniczenie nadzoru doprowadziło do zdefiniowania zbioru zasad przyjętych następnie w demokratycznym świecie w ramach krajowej, lokalnej i międzynarodowej legislacji. Przez pewien czas wydawało się, że Internet dokona redemokratyzacji społeczeństwa. Medium, które pierwotnie postrzegane było jako anonimowe, stało się jednak dzięki rewolucji cyfrowej narzędziem wykorzystywanym w przetwarzaniu danych osobowych, nieobojętnym dla interesów użytkowników Internetu. Dążenie do pozyskania możliwie największej wiedzy o osobie stało się nie tylko podstawą strategii biznesowych takich gigantów jak Google, Facebook & Twitter, lecz także batalii prowadzonej przez demokratyczne państwa przeciwko terroryzmowi i w wojnie cybernetycznej. Celem niniejszego opracowania jest zwrócenie uwagi na łatwość, z jaką różne grupy (grupa lobbingowa, partia polityczna, rząd) mogą oddziaływać za pomocą kluczowych informacji, wykorzystując w tym celu tzw. efektu komory echa. Wiele państw zaczęło ograniczać zasady prawne, zagrażając tym samym prywatności i innym ważnym prawom człowieka. Ryzyko z tym związane będzie poddane pod dyskusję.

## How the Internet changes the Legal Framework of Privacy?


### Summary

The concept of privacy and the limitation of surveillance once have involved a well established set of principles adopted around a democratic world of national, sub-national and international laws and jurisdictions. For a time, it seemed that even the Internet was going to redemocratize society. But what once has been an anonymous medium becomes within the digital revolution a tool of personal data, opaque to the interest of Internet users. The race to know as much as possible about a person has become the central issue not only in the business strategy of the inter giants like Google, Facebook & Twitter, but also in the battle against terrorism and cyberwar by democratic states. In the following paper it should be seen how easily anything with an agenda (a lobbying group, a political party, a government) could flood the echo chamber with information central to its cause. Many of them have begun to chip away at its legal principles, endangering privacy and other important human rights. This risk will be discussed.