PANOPTYKON
F U N D A C J A

OCHRONA PRYWATNOŚCI W WARUNKACH SPOŁECZEŃSTWA INFORMACYJNEGO: DIAGNOZA PROBLEMU, PROPOZYCJE ZMIAN

Główne tezy

Przemiany, które obserwujemy w sferze technologii oraz relacji społecznych niosą ze sobą nowe zagrożenia dla praw i wolności obywateli. Prawo do prywatności wydaje się na tym tle szczególnie zagrożone ze względu na wzrost ilości narzędzi umożliwiających ingerowanie w tę sferę oraz poszerzające się spektrum potencjalnych naruszeń.

Nowoczesne technologie nie tylko ułatwiają i wzbogacają komunikację między ludźmi; pozwalają także **zbierać i przetwarzać coraz więcej informacji** o naszym życiu oraz, co kluczowe, **łączyć je ze sobą**. Dzieje się to w sposób zautomatyzowany i coraz mniej zauważalny dla przeciętnego obywatela. Brakuje społecznej świadomości i wiedzy w tym zakresie, co koresponduje z ograniczonym zainteresowaniem problematyką ochrony prywatności i nowych form nadzoru po stronie mediów. W efekcie procesy i zjawiska umożliwiające coraz głębszą ingerencję w sferę naszej prywatności (w tym zmiany prawne), pozostają w dużej mierze poza kontrolą społeczeństwa. Zmienia się wreszcie samo rozumienie prywatności i przesuwają granice tego, co uznajemy za dopuszczalne.

Za tymi zmianami niewątpliwie nie nadąża prawo, instytucje powołane do ochrony praw obywatelskich i polityka państwa. Prywatność obywateli nie jest w dostateczny sposób chroniona, zarówno w odniesieniu do działań podejmowanych przez instytucje państwowe, jak i wobec praktyk podmiotów komercyjnych, gromadzących ogromne ilości danych. Wreszcie, obywatele często nie wiedzą jak reagować, kiedy czują, że ich prawa w tej sferze są naruszane, ani gdzie szukać realnej pomocy. Ta sytuacja wymaga zmian prawnych i instytucjonalnych.

PRÓBA DIAGNOZY

1. Co się zmienia w sferze technologii?

Dążenie do coraz ściślejszego nadzoru nad społeczeństwem realizuje się przede wszystkim dzięki powszechnej dostępności nowych technologii, umożliwiających gromadzenie i przetwarzanie ogromnej ilości danych. Kluczowe jest przy tym zautomatyzowanie procesu pozyskiwania danych i jego niezauważalny charakter: obywatele często nie zdają sobie sprawy z cyfrowych śladów, jakie po sobie pozostawiają, czy sposobów, w jakie rozmaite instytucje mogą pozyskiwać informacje o ich życiu.

Poniżej przytaczamy kilka przykładów ilustrujących ogrom możliwości, jakie pojawiły się w tej sferze.

Telekomunikacja (np. Internet, telefonia komórkowa, usługi VoIP) to sfera, w której przepływ informacji jest poddawany coraz ściślejszej kontroli. Z jednej strony, mamy do czynienia z obowiązkami w zakresie retencji danych nakładanymi na prywatnych operatorów przez organy państwa oraz szerokim dostępem służb specjalnych do tych informacji. Z drugiej, niedoskonałość prawa i nieświadomość użytkowników jest skrupulatnie wykorzystywana przez podmioty komercyjne (dzięki przeglądarkom, wyszukiwarkom, portalom społecznościowym, sklepom Internetowym) do gromadzenia informacji o naszej aktywności w Internecie. Do tych zagrożeń dochodzi technologia GPS umożliwiająca dokładną lokalizację każdego posiadacza telefonu komórkowego.

Biometria – jako technika identyfikacji – wchodzi do powszechnego użycia zarówno w sferze publicznej, jak i prywatnej. Od zeszłego roku funkcjonują w Polsce roku paszporty z dwiema cechami biometrycznymi; rząd wycofał się ostatnio z pomysłu wykorzystania danych biometrycznych w dowodach osobistych, ale nie jest przesądzone, czy ta koncepcja nie wróci. Mocno promowany jest pomysł rozpowszechnienia w Polsce biometrycznych bankomatów. Coraz częściej dane biometryczne są wykorzystywane przez pracodawców do kontroli czasu pracy. Zdarzają się nawet tak kuriozalne przypadki, jak wykorzystywanie odcisków palców do sprawdzania obecności na mszy młodzieży przystępującej do sakramentu bierzmowania.

Monitoring wizyjny rozwija się w Polsce w sposób niezwykle dynamiczny, czemu sprzyja stosunkowo niski koszt tych urządzeń oraz dość powszechna (choć mało uzasadniona) wiara w ich skuteczność w zapewnianiu bezpieczeństwa. Problem dotyczy

przede wszystkim systemów prywatnych, które wymykają się regulacjom prawnym: kamery montowane są na wielką skalę i bez rozróżnienia na typ monitorowanej przestrzeni (pojawiają się w toaletach i przebieralniach); nie wiadomo też, jak długo nagrania są przechowywane i kto ma do nich dostęp. Jednak nawet w tych sferach, które są poddane regulacji – jak monitoring wizyjny w więzieniach i szkołach – jego użycie i wszechobecność budzi poważne zastrzeżenia („legalnie" monitorowane są nawet miejsca przeznaczone do czynności intymnych).

Na tym tle pojawia się pytanie o znaczenie i społeczne konsekwencje rozwoju technologii: czy rzeczywiście, z punktu widzenia praw człowieka, technologia jest tylko neutralnym narzędziem? Na ile sam jej rozwój prowadzi do zwiększenia lub zmiany form nadzoru nad ludźmi?

2. Czemu i komu mogą służyć współczesne technologie nadzoru?

Z technologii umożliwiających gromadzenie i wymianę danych na masową skalę korzystają państwa, instytucje ponadpaństwowe, takie jak Unia Europejska, i podmioty komercyjne. Różnią się tylko cele i skala nadzoru.

Sfera publiczna: nowe rejestry, większa interoperacyjność i wymiana danych, integracja baz

Generalnym trendem, który da się zaobserwować w działaniach instytucji publicznych, jest **zbieranie coraz większej liczby informacji o obywatelach**. Mamy poszerzający się obowiązek retencji danych telekomunikacyjnych dla celów bezpieczeństwa; plany rozszerzenia zestawu pytań w kolejnym spisie powszechnym; czy takie subtelne narzędzia gromadzenia danych, jak funkcjonujące w wielu miastach spersonalizowane karty miejskie (często rejestrujące dane geolokalizacyjne).

Kluczowe z punktu widzenia efektywności zarządzania informacją jest tworzenie systemów opartych na pełnej **interoperacyjności.** Digitalizacja oraz zorganizowanie zbiorów w oparciu o ten sam klucz (np. numer PESEL) umożliwiają natychmiastowy dostęp do danych i wymianę informacji. Ten proces realizuje się nie tylko na poziomie państwa (np. w ramach projektu pl.ID), ale także na poziomie międzynarodowym, np. w ramach zacieśniania współpracy między służbami specjalnymi w Unii Europejskiej (system SIS II).

Pojawiają się także plany tworzenia rozmaitych **„superbaz"**, w których mają być przechowywane ogromne ilości danych, np. zintegrowana baza danych medycznych i informacji o pobieranych świadczeniach społecznych (NFZ, MPiPS oraz ZUS) czy baza, która ma powstać na podstawie najbliższego spisu powszechnego.

Wreszcie, nie można pominąć działalności służb specjalnych, których możliwości w zakresie pozyskiwania danych są ogromne. Wymieńmy tylko: stosowanie podsłuchów operacyjnych, dostęp do rejestrów publicznych, prawo dostępu do danych retencyjnych w celach prewencyjnych (a zatem bez związku z konkretnym postępowaniem). Mimo tak szerokich uprawnień, praktyka służb nierzadko ociera się o działania pozaprawne (np. wymiana danych między ZUS-em a służbami, podsłuchiwanie dziennikarzy przez ABW i wykorzystanie tych materiałów w procesie cywilnym).

Sfera prywatna: bazy klientów, inwigilacja pracowników, wszechobecny monitoring

Problem zbierania coraz większej ilości informacji dotyczy również podmiotów prywatnych. **Dane o nas – jako klientach – posiada** niemal każda firma, która świadczy na naszą rzecz najdrobniejszą nawet usługę. Są to nie tylko operatorzy komórkowi, linie lotnicze, banki czy firmy ubezpieczeniowe, ale także księgarnie, pizzerie, korporacje taksówkowe i setki firm trudniących się marketingiem bezpośrednim. Powszechne korzystanie z Internetu i bankowości elektronicznej odgrywa w tym procesie kluczową rolę: to dzięki naszym **„cyfrowym śladom"**, pozostawianym na każdym kroku, można z taką łatwością pozyskiwać cenne dane i generować precyzyjne profile marketingowe.

Podobnie **jako pracownicy jesteśmy coraz częściej poddawani przez pracodawców permanentnej inwigilacji**. Wykorzystywane są do tego celu coraz bardziej zaawansowane metody: elektroniczne monitorowanie czasu pracy, kamery przemysłowe, kontrola działań w Internecie oraz rozmów telefonicznych czy testy psychologiczne.

3. Dlaczego polskie społeczeństwo pozostaje zazwyczaj bierne?

Tendencja do zwiększania kontroli nad obywatelami w imię potrzeby zapewnienia bezpieczeństwa jest zjawiskiem dość powszechnym i dotyczy wielu krajów. Różnica między Polską a wieloma państwami tzw. starej Europy polega na tym, że tam procesy te zostały już dość dobrze zdiagnozowane (koncepcja *surveillance society*) i są przedmiotem badań (*surveillance studies*) oraz monitoringu obywatelskiego. Tymczasem w Polsce **brakuje nawet języka do opisu zachodzących zmian**. Jeśli nawet w debacie publicznej pojawiają się doniesienia o konkretnych nadużyciach związanych z nadzorem, nie są one analizowane w szerszym kontekście zmian społecznych.

Deficytowi systemowej analizy tych nowych zjawisk towarzyszy **brak szerszej społecznej świadomości problemu**. Większość obywateli nie wiąże zagrożeń dla swojej prywatności z postępującym rozwojem technologii służących nadzorowi. Natomiast osoby dotknięte realnymi nadużyciami bardzo często nie wiedzą, jak reagować, do jakiej instytucji zwrócić się o pomoc, jak dochodzić realizacji swoich praw. W rezultacie można mówić o deficycie demokratycznej kontroli nad funkcjonowaniem współczesnych systemów nadzoru w Polsce.

Możemy również zaobserwować dość powszechne **społeczne przyzwolenie na daleko idące ograniczenia wolności i prywatności** w imię bezpieczeństwa bądź wygody. Czy ma to związek z niskim poziomem wzajemnego zaufania lub brakiem poczucia bezpieczeństwa? Aby stwierdzić, na ile taka hipoteza jest słuszna, potrzeba oczywiście systematycznych i pogłębionych badań. Można jednak zaryzykować tezę, że obecny stan ma związek z doświadczeniami życia w świecie realnego socjalizmu i czasu transformacji. Z jednej strony, Polacy przez lata funkcjonowania w poprzednim systemie oswoili się z wszechogarniającą kontrolą, przyjmując ją jako zjawisko poniekąd naturalne. Z drugiej strony, w latach 90. mogło dojść do odreagowania i swoistego zachłyśnięcia się nową, demokratyczną rzeczywistością, w której nie ma już jawnie opresyjnej władzy, a jednostka teoretycznie znalazła się w centrum systemu prawnego. Zmiany w zakresie praw człowieka w ciągu ostatnich 20 lat koncentrowały się na wyzwaniach transformacji ustrojowej, podczas gdy w Europie Zachodniej poważnie dyskutowano na temat zagrożeń związanych z rozwojem nowych technologii.

Zapewne dopiero uczymy się funkcjonować w świecie kreowanych przez media niebezpieczeństw i paniki moralnej. Rola środków masowego przekazu w generowaniu poczucia zagrożenia i definiowaniu wrogów społeczeństwa wydaje się kluczowa. Dlatego są one narzędziem, za pomocą którego realizowana jest **polityka strachu**. Szafowanie argumentem bezpieczeństwa przekłada się w Polsce na wysokie poparcie wyborcze, a jednocześnie przynosi zyski biznesowi bezpieczeństwa. Podejmowane działania nie zawsze są jednak odpowiedzią na realne zagrożenia, natomiast służą jako pretekst do zwiększenia kontroli nad obywatelami: w imię zasady, że **każdy jest potencjalnie podejrzany**.

Badania pokazują, że zaufanie społeczne i poczucie bezpieczeństwa wśród polskiego społeczeństwa zaczyna w ostatnich latach wzrastać. Mimo to polityka strachu nadal wydaje się skutecznym narzędziem politycznym i marketingowym. Choć pojawiają się również optymistyczne symptomy zmian. Jednym z nich może być społeczny protest wywołany projektem wprowadzenia w Polsce Rejestru Stron i Usług Niedozwolonych. Argumentacja, że walka z pedofilią i nielegalnym hazardem usprawiedliwia nawet Najdalej idące działania państwa nie spotkała się z akceptacją sporej części polskiego społeczeństwa.

Czynniki historyczne, specyficzne dla naszego kraju czy regionu, nakładają się na głębsze przemiany społeczne, obejmujące między innymi ewolucję samego pojęcia prywatności. Rozwój współczesnych narzędzi komunikacji i wymiany informacji wpływa na postępujące rozmycie granic między sferą intymną człowieka a sferą społeczną; między tym, co uznajemy za dopuszczalne, a tym, co odczuwamy jako ingerencję w naszą prywatność.

4. Dlaczego prawo nie chroni w dostateczny sposób naszej prywatności?

Przede wszystkim prawo bywa wykorzystywane przez władzę publiczną do zwiększania kontroli nad obywatelami. Kolejne **zmiany prawa idą w kierunku zwiększania ilości gromadzonych informacji** oraz możliwości ich wykorzystywania przez instytucje publiczne. W ramach przykładów warto przywołać chociażby aktualne oraz postulowane uprawnienia służb specjalnych, próby zwiększenia kontroli nad przestrzenią Internetu, retencję danych telekomunikacyjnych, plany integracji publicznych baz danych w ramach projektu pl.ID i rozbudowy bazy GUS-u, a także rozwoju i centralizacji elektronicznych baz danych medycznych.

Wiele zmian prawnych prowadzących do ściślejszego nadzoru nad społeczeństwem stanowi konsekwencję wdrażania do polskiego porządku prawnego rozwiązań przyjmowanych w **Unii Europejskiej** (np. dane biometryczne w paszportach, retencja danych telekomunikacyjnych). Zdarza się jednak, że **władza wykorzystuje implementację unijnych przepisów do wdrożenia jeszcze dalej idących rozwiązań** (tak było np. w przypadku retencji danych); często przedstawiając je jako prostą realizację obowiązków nałożonych przez Unię Europejską.

Na te problemy nakłada się **mała przejrzystość procesu legislacyjnego**, wprowadzenie rozwiązań ograniczających konstytucyjne prawa za pomocą aktów niższej rangi czy „przy okazji" rozproszonych nowelizacji, przekraczanie delegacji ustawowych, czy wreszcie duży wpływ służb specjalnych na tworzenie prawa. Efektywny protest społeczny przeciwko rozwiązaniom prawnym wprowadzanym w taki sposób jest w praktyce bardzo utrudniony, o ile nie w ogóle niemożliwy.

Oczywiście naruszenia prawa do prywatności nie wynikają jedynie z działalności instytucji publicznych. Ich źródłem są bardzo często działania podmiotów i osób prywatnych. Problem nasila się wraz z rozwojem społeczeństwa informacyjnego. Szybkość i wielokierunkowość obiegu danych sprawia, że **informacja naruszająca prywatność zaczyna bardzo szybko żyć własnym życiem**. To stawia przed organami ochrony prawnej **wyzwanie sprawnego reagowania na naruszenia prawa.** Tymczasem regulacje prawne z zasady nie nadążają za zmianami technologicznymi. Dotyczy to chociażby naruszeń dokonywanych przy wykorzystaniu Internetu czy problemów wynikających z braku kompleksowej regulacji funkcjonowania monitoringu wizyjnego. Zdarza się również, że naruszenie prawa jest oczywiste, brakuje jednak instrumentów, które pozwoliłyby jednostce na szybką i skuteczną ochronę. W tym zakresie **państwo wydaje się nie spełniać roli gwaranta realizacji praw na poziomie horyzontalnym.**

Wszystko to coraz częściej prowadzi do ograniczania praw i wolności jednostki: nie tylko prawa do prywatności i autonomii informacyjnej, ale także ograniczenia wolności, naruszenia godności i praktyk dyskryminacyjnych. Mają one miejsce zarówno w relacji państwo-obywatel, jak i w relacjach między prywatnymi podmiotami, wtedy kiedy państwo nie jest w stanie zapewnić słabszej stronie efektywnej ochrony prawnej.

Warto także dodać, że stopniowe zrzekanie się naszej prywatności na rzecz większej funkcjonalności państwa jest drogą bez powrotu. Trudno sobie wyobrazić powrót do stanu sprzed "utraconej wolności". Dlatego tak ważna jest szczególna dbałość o poszanowanie standardów stanowienia prawa czy niedopuszczalność określonych praktyk, zanim władze publiczne zbiorą odpowiednie dane i stworzą kolejny rejestr.

PROPOZYCJE ZMIAN

1. Reforma instytucjonalna GIODO

- **Zweryfikowanie kompetencji i uprawnień** GIODO pod kątem skutecznej realizacji prawa do kontroli przetwarzania danych (uzyskiwania wyczerpującej informacji na temat tego, kto i w jakim celu przetwarza nasze dane).
- **Poszerzenie uprawnień rzeczniczych GIODO,** w szczególności o prawo domagania się w imieniu obywateli sprawnego i szerszego dostępu do informacji; **Alternatywnie:** utworzenie odrębnej instytucji rzecznika ds. informacji.
- Umożliwienie obywatelom i organizacjom społecznym domagania się od GIODO abstrakcyjnej kontroli przetwarzania danych w interesie publicznym.
- Nadanie GIODO prawa wnoszenia skargi do Trybunału Konstytucyjnego.
- Nadanie GIODO możliwości nakładania kar finansowych za niektóre naruszenia ustawy o ochronie danych osobowych.
- Poddanie kontroli GIODO działań kościołów i związków wyznaniowych w zakresie przetwarzania danych osobowych.
- Zweryfikowanie zakresu uprawnień kontrolnych GIODO w odniesieniu do przetwarzania danych przez służby specjalne.

2. Uporządkowanie przepisów prawa

- Przeprowadzenie audytu istniejących procedur, umożliwiających obywatelom kontrolę przetwarzania danych, pod kątem ich skuteczności i realności.
- Zweryfikowanie, czy przepisy (obecnie rozproszone) regulujące prawo obywateli do informacji i kontroli nad swoimi danymi nie powinny zostać zebrane w jednej, odrębnej ustawie, tak aby ujednolicić procedury i ułatwić korzystanie z nich.
- Wprowadzenie kompleksowej regulacji stosowania monitoringu wizyjnego, w szczególności przez podmioty prywatne.
- Zagwarantowanie, w formie odpowiednich regulacji prawnych, ochrony prywatności obywateli w związku z planowaną integracją publicznych rejestrów.
- Zweryfikowanie uprawnień służb specjalnych w zakresie niejawnego dostępu do danych, w szczególności w zakresie działań prewencyjnych.

3. Poszerzenie dostępu do informacji nt. danych zbieranych przez służby specjalne

Nałożenie na służby obowiązku regularnego publikowania informacji statystycznej na temat stosowanych niejawnych metod pozyskiwania danych o obywatelach (podsłuchy, dostęp do danych retencyjnych, geolokalizacja, dostęp do rejestrów publicznych oraz baz prywatnych), w szczególności na temat liczby wniosków, zgód i odmów oraz powoływanych podstaw prawnych, w rozbiciu na poszczególne służby.

4. Edukacja obywatelska

Przygotowanie szerokiej kampanii informacyjnej na temat tego, jak obywatele mogą realizować swoje prawo do prywatności w rzeczywistości społeczeństwa informacyjnego oraz przygotowanie przystępnego kompendium wiedzy, dostępnego w Internecie.