

Raport o społeczeństwie nadzorowanym

Sporządzony przez Surveillance Studies Network dla Rzecznika ds.
Informacji

Wrzesień 2006 r.

Raport pełny

Autorzy

Redaktor:

David Murakami Wood

Autorzy raportu:

**Kirstie Ball
David Lyon
David Murakami Wood
Clive Norris
Charles Raab**

Autorzy raportów specjalistycznych:

**Louise Amore
Kirstie Ball
Stephen Graham
Nicola Green
David Lyon
Jason Pridmore
Clive Norris
Charles Raab
Ann Rudinow Saetnan**

Krytycy:

**Sarah Earle
Graham Sewell**

Materiały dodatkowe:

Emily Smith

Wsparcie administracyjne:

Anne Fry

Rozwój projektu:

Mark Siddoway / Knowledge House

Spis treści

Część	Tytuł
Część A	Wprowadzenie do społeczeństwa nadzorowanego
1	Społeczeństwo nadzorowane: streszczenie, historia, definicje
2	Co jest nie tak ze społeczeństwem nadzorowanym?
3	Definicja nadzoru, śledzenie społeczeństwa nadzorowanego
4	Perspektywy dotyczące społeczeństwa nadzorowanego 1: problemy
5	Perspektywy dotyczące społeczeństwa nadzorowanego 2: procesy
6	Przewodnik po raporcie
Część B	Badanie społeczeństwa nadzorowanego
7	Wprowadzenie
8	Kontekst społeczeństwa nadzorowanego
9	Technologie nadzoru
10	Procesy nadzoru
11	Społeczne konsekwencje nadzoru
Część C/1	Tydzień z życia w społeczeństwie nadzorowanym w 2006 r.
12	Wprowadzenie
13	Na lotnisku
14	Zakupy
15	W domu
16	Na mieście
17	Przestępczość a społeczeństwo
18	Biuro obsługi klienta
19	Zdrowie
20	Szkoła i po...
21	Rodzina
22	Znowu w biurze obsługi klienta
23	Oszustwo
23	Z powrotem na mieście
25	Wniosek
Część C/2	Obrazy z życia w społeczeństwie nadzorowanym, rok 2016
26	Wstęp
27	Kontrola tożsamości
28	Przejścia graniczne
29	Zarządzanie zestawem otaczających nas marek (krajobrazami marek)
30	Bezgotówkowe zakupy
31	Mieć dzieci na oku
32	Totalne rozwiązania społeczne?
33	Zmiana zasad jazdy
34	Przyjazne, latające oczy na niebie
35	Niezidentyfikowana pod-klasa
36	Wirtualne śledzenie
37	Twoje życie to nasza sprawa
38	Troska o ciebie
39	Wnioski : lustrzany korytarz

CzęśćD	Regulowanie społeczeństwa nadzorowanego
40	Wprowadzenie
41	Co jest nie tak z regulowaniem?
42	Obecny stan regulacji
43	Instrumenty regulacyjne: wady i zalety
44	Ogólne problemy dotyczące instrumentów
45	Możliwości rozwoju prawodawstwa

Część A: Wprowadzenie do społeczeństwa nadzorowanego

1. Społeczeństwo nadzorowane: streszczenie, historia, definicje

- 1.1. Żyjemy w społeczeństwie nadzorowanym. Społeczeństwo nadzorowane już funkcjonuje. We wszystkich bogatych państwach świata życie codzienne jest pełne przypadków nadzoru, nie tylko od rana do wieczora, lecz przez całą dobę i 7 dni w tygodniu. Niektóre z tych przypadków zakłócają ustalony porządek dnia, jak kiedy dostajemy mandat za przejechanie na czerwonym świetle, chociaż jedynym świadkiem jest kamera. Jednak większość z nich stanowi obecnie element składowy naszej codzienności, którego nawet nie zauważamy.
- 1.2. Myślenie w kategoriach społeczeństwa nadzorowanego oznacza wybranie pewnego punktu widzenia, oznacza pewien sposób patrzenia na współczesny świat. Oznacza mówienie głośno nie tylko o tych codziennych przypadkach, kiedy spotykamy się z nadzorem, ale również o potężnych systemach nadzoru, które obecnie stanowią fundament nowoczesnego społeczeństwa. Nie chodzi jedynie o to, że kamery telewizji przemysłowej (CCTV) mogą nas sfilmować kilkaset razy dziennie, że musimy pokazywać nasze karty lojalnościowe ochroniarzowi przy wejściu do supermarketu albo że musimy mieć kodowaną kartę dostępu, aby dostać się rano do biura. Chodzi o to, że systemy nadzoru reprezentują elementarną skomplikowaną infrastrukturę, u której podstaw leży założenie, że gromadzenie i przetwarzanie naszych danych osobowych jest niezbędnym elementem współczesnego modelu życia.
- 1.3. Przyjęło się utożsamiać mówienie o społeczeństwie nadzorowanym z opowiadaniem o sprawach mrocznych, mających coś wspólnego z dyktatorami i totalitaryzmem. Do Wielkiego Brata przejdziemy za chwilę, ale społeczeństwo nadzorowane należy raczej rozumieć jako produkt nowoczesnych praktyk organizacyjnych, nowoczesnych przedsiębiorstw, rządów i nowoczesnego wojska, a nie potajemnego spisku. Nadzór można uważać za rozwój w kierunku wydajnej administracji, z korzyścią, zdaniem Maxa Webera, dla rozwoju zachodniego kapitalizmu i nowoczesnego narodu i państwa.¹
- 1.4. Niektóre formy nadzoru istniały zawsze, tak jak zawsze ludzie obserwowali się nawzajem w ramach wzajemnej opieki, kontroli moralności lub zdobywania informacji. Jednakże około 400 lat temu do praktyk organizacji zaczęto stosować metody „racjonalne”, co przyczyniło się do stopniowej likwidacji nieformalnych sieci społecznych i zasad, w oparciu o które wcześniej prowadzono działalność gospodarczą i rządzono krajami. Normalne więzi społeczne przestały mieć znaczenie, dzięki czemu powiązania rodzinne i tożsamość jednostek nie stanowiły już przeszkody dla płynnego funkcjonowania tych nowych organizacji. Dobrą wiadomością było jednak to, że dzięki temu obywatele, a ostatecznie także i pracownicy mogli się teraz spodziewać respektowania swoich praw, jako że zaczęli być chronieni dzięki szczegółowym nagraniom, jak przepisami prawa.

¹ Gerth, H. i Wright Mills, C. (1964) "From Max Weber [Z Maxa Webera]", New York.

- 1.5. Po drugiej wojnie światowej, kiedy naród i państwo kwitły a urzędy mnożyły się, obciążone systemy zaczęły trzeszczeć a nawet pękać w szwach. Jednak w zasięgu ręki była pomoc w postaci nowych systemów komputerowych, które pozwoliły zmniejszyć nakład siły roboczej i zwiększyć niezawodność i ilość pracy, która mogła zostać wykonana. Z czasem, dzięki nowym systemom komunikacji, znanym obecnie pod łączną nazwą „techniki informacyjnej” (IT), administracja biurowa mogła być prowadzona nie tylko pomiędzy różnymi wydziałami tej samej organizacji, ale również pomiędzy różnymi organizacjami, a wreszcie również pomiędzy różnymi państwami. Podobnie działo się w przypadku działalności gospodarczej: początkowo prowadzono rejestry, potem tworzone sieci, a następnie zaczęto działać na skalę globalną – dzięki technice informacyjnej. Jednak nawet takie „połączone” działania mają związek z technicznym i nowoczesnym pędem ku wydajności, szybkości, kontroli i koordynacji.
- 1.6. Nadzór rozprzestrzenił się za sprawą bezosobowych praktyk, którymi rządzą konkretne zasady. Istotą biurokracji jest nadzór nad podwładnymi i tworzenie rejestrów w ramach systemu. Zwyczaje firm polegające na podwójnym księgowaniu i próbach cięcia kosztów i podnoszenia zysków przyspieszyły i umocniły zjawisko nadzoru tego rodzaju, co wpłynęło na życie zawodowe i konsumpcję. Miało to również wpływ na rozrastanie się urzędów wojskowych i policyjnych w XX wieku, napędzane gwałtownym rozwojem nowych technologii, ulepszonymi metodami gromadzenia informacji wywiadowczych, technikami identyfikacji i śledzenia. Jednak najistotniejsze jest to, że coraz intensywniejszy nadzór stanowi element nowoczesności.

2. Co jest nie tak ze społeczeństwem nadzorowanym?

- 2.1. Rozumienie społeczeństwa nadzorowanego jako produktu nowoczesności pomaga uniknąć dwóch istotnych pułapek: myślenia o nadzorze jako o spisku uknutym przez złe moce oraz myślenia, że nadzór jest wyłącznie rezultatem nowych technologii (najwięksi paranoicy oczywiście wpadają w obydwie pułapki jednocześnie). Jednak postrzeganie nadzoru we właściwej perspektywie jako wyniku biurokracji i dążenia do skuteczności, szybkości, kontroli i koordynacji nie oznacza, że wszystko jest w porządku. Oznacza to, że należy być ostrożnym w identyfikowaniu kwestii kluczowych i czujnym przy zwracaniu na nie uwagi.
- 2.2. Nadzór ma dwa oblicza, należy uznać również jego korzyści. Jednocześnie jednak w systemach zaprojektowanych na wielką skalę stale obecne jest ryzyko oraz zagrożenia, a władza oczywiście korumpuje lub przynajmniej zmienia perspektywę tych, którzy ją posiadają.
- 2.3. Zajmijmy się najpierw ryzykiem i zagrożeniami. Są czymś, do czego się przyzwyczailiśmy, kiedy w końcu dwudziestego wieku zdaliśmy sobie sprawę, że „postęp” nie jest jednoznacznym błogosławieństwem. Każdy wzrost produkcji „dóbr” (*goods*), jak to zwięźle ujmuje Ulrich Beck², oznacza także większą produkcję „rzeczy złych” (*bads*).³
- 2.4. Poza „złem” środowiskowym, o którym Beck mówi przede wszystkim, jest jeszcze między innymi zło społeczne i polityczne. Infrastruktury technologiczne działające na wielką skalę szczególnie sprzyjają problemom na wielką skalę.

² Beck, U. (1992) *The Risk Society [Społeczeństwo ryzyka]*, Newbury Park CA: Sage.

³ Nieprzetłumaczalna gra słów: *goods* (dobro w liczbie mnogiej lub towary) / *bads* (zło w liczbie mnogiej) – przyp. tłum.

Szczególnie w przypadku systemów komputerowych, naciśnięcie klawisza przez nieuwagę lub z wyniku niedoinformowania może łatwo spowodować katastrofę. Jako przykład można podać ujawnienie w sierpniu 2006 r., dla celów „naukowych”, zapytań *on-line* wysłanych za pośrednictwem AOL przez dwadzieścia milionów zwykłych ludzi. Wydaje się, że zapytania nie były opatrzone żadnymi identyfikatorami, a jednak tylko kilka chwil zajęło rozpoczęcie dopasowywania wyników wyszukiwania do odpowiednich osób.⁴ Niniejszy raport porusza kilka problemów systemów nadzoru na wielką skalę.

- 2.5. Należy także pamiętać o korupcji i skrzywionym postrzeganiu władzy. I znów, aby zrozumieć problem nie trzeba wyobrażać sobie tyrana próbującego uzyskać dostęp do baz danych ubezpieczeń społecznych czy baz danych medycznych. Korupcja władzy dotyczy decydentów, którzy obiecują większe korzyści (jak zwycięstwo w wojnie) w celu uzasadnienia zastosowania wyjątkowych lub nadzwyczajnych środków.
- 2.6. W Stanach Zjednoczonych podczas drugiej wojny światowej Amerykanie japońskiego pochodzenia byli identyfikowani i internowani dzięki wykorzystaniu danych ze spisów powszechnych, co normalnie jest bezprawne. Jako bardziej aktualny przykład można podać ograniczanie możliwości podróżowania wielu muzułmanom amerykańskim, których nazwiska znajdują się na listach osób nie wpuszczanych do samolotów, lub inne przypadki dyskryminacji rasowej niedopuszczalnej w innych sytuacjach ze względu na oczywistą niesprawiedliwość.⁵ O ile biali Amerykanie mogą unikać opóźnień na lotniskach poprzez wprowadzenie niewielkich zmian w nazwiskach podczas rezerwacji lotów, w przypadku ludzi, których nazwiska brzmią „arabsko” lub „muzułmańsko” jest to dużo trudniejsze.⁶ Wszelkie „okoliczności wyjątkowe”, szczególnie jeżeli chodzi o wyjątki, które obowiązują stale jak w przypadku niekończącej się „wojny z terroryzmem” to te, które wymagają specjalnej czujności obrońców praw człowieka i obywatela.
- 2.7. Poza tym, w świecie zaawansowanej technologii i handlu światowego niepożądane konsekwencje działań podejmowanych w dobrej wierze pojawiają się bardzo często. Na przykład, w trosce o konkurencyjność, przedsiębiorstwa „znają swoich klientów”, jak nam się mówi i organizują ukierunkowane kampanie reklamowe, a nawet wybierają odpowiednie lokalizacje na zakłady i sklepy. Nikt nie pomyśli, że kierownik sklepu, który chce przyciągnąć jak najbardziej wiarygodnych klientów działa niewłaściwie decydując się na sprawdzanie ich wypłacalności za pośrednictwem instytucji informacji kredytowej. Ma to po prostu znaczenie dla większego zysku. Jednak rezultatami – niepożądanymi konsekwencjami – wykorzystywania danych w celu zapewnienia sobie dochodowych klientów jest preferencyjne traktowanie pewnych grup, oparte na zdolności finansowej, a wykluczenie innych grup.⁷

⁴ Zob.: Barbaro, A. and Zeller, T. „A face is exposed for AOL searcher no. 4417749 [Pokazano twarz użytkownika AOL nr 4417749]”, *New York Times*, 9 August 2006. <http://select.nytimes.com/gst/abstract.html?res=F10612FC345B0C7A8CDDA10894DE404482/>

⁵ Zob.: Amnesty International USA (2004) *Threat and Humiliation: Racial Profiling, Domestic Security and Human Rights in the USA* [Zagrożenie i poniżenie – profilowanie rasowe, bezpieczeństwo wewnętrzne i prawa człowieka w USA], New York: Amnesty International USA, http://www.amnestyusa.org/racial_profiling/report/rp_report.pdf

⁶ Kehaulani Goo, S., „Hundreds Report Watch-List Trials [Setki procesów o listy nadzoru]” 21 sierpnia 2004, <http://www.washingtonpost.com/ac2/wp-dyn/A20199-2004Aug20?language=printer>

⁷ Lace, S (2005) *The Glass Consumer* [Szklany konsument], Bristol UK: Policy Press; Danna, A. and Gandy, O. (2002) „All that glitters is not gold: Digging beneath the surface of data-mining [Nie wszystko złoto co się świeci. Pod powierzchnią analizy danych]” *Journal of Business Ethics*, 40: 373-386; Lyon, D. (ed.) (2003) *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* [Nadzór jako sortowanie społeczne – prywatność, ryzyko i dyskryminacja cyfrowa], London and New York: Routledge.

2.8. Problemy wiążące się ze społeczeństwem nadzorowanym obejmują jeszcze trzy inne elementy.

2.8.1. Pierwszy dotyczy okoliczności wyjątkowych i niepożądanych konsekwencji. Konieczne jest szczegółowe zbadanie systemów, które sankcjonują znaczną nierówność dostępu i możliwości rozwoju. Jest to oczywiście trudne w sytuacji, gdy celem wszystkich prawdziwych systemów nadzoru jest odmienne traktowanie różnych grup, ale przynajmniej można unaocznnić ten problem. Niestety dominujące kierunki rozwoju metod nadzoru w dwudziestym pierwszym wieku powodują sytuacje, w których sposoby rozróżniania klasy, rasy, płci, pochodzenia geograficznego i obywatelstwa jest obecnie zastrzane i instytucjonalizowane. Nasz raport je wyszczególnia.

2.8.2. Drugą kwestią, mającą szczególne znaczenie dla spójności i solidarności społecznej jest to, że wszystkie obecne procesy i praktyki nadzoru wskazują, że żyjemy w świecie pozbawionym zaufania. Nadzór sprzyja podejrzliwości.⁸ Pracodawca, który instaluje urządzenia odnotowujące każde naciśnięcie klawisza na klawiaturze lub urządzenia GPS w samochodach służbowych przyznaje, że nie ufa swoim pracownikom. Pracownik opieki społecznej, który szuka dowodów na korzystanie z kilku świadczeń lub próbuje zdobyć informacje od sąsiadów przyznaje, że nie ufa odbiorcom świadczeń. A kiedy rodzice zaczynają korzystać z kamer internetowych i systemów GPS do kontrolowania swoich dzieci, także przyznają, że im nie ufają. Można powiedzieć, że niektóre z tych działań to po prostu ostrożność. Ale jak daleko może to zajść? Relacje społeczne opierają się na zaufaniu i pozwalanie na jego osłabianie w ten sposób to powolne społeczne samobójstwo.

2.8.3. Kolejna wątpliwość dotycząca społeczeństwa nadzorowanego wiąże się z obawą, że nadzór, szczególnie ten związany z zaawansowanymi technologiami i walką z terroryzmem, odwraca uwagę od alternatywnych rozwiązań oraz od istotniejszych i bardziej pilnych kwestii. Można się zastanawiać, czy to naprawdę jest najlepszy sposób na osiągnięcie tych celów. Niestety, bez popadania w cynizm należy zauważyć, że stosowanie nowoczesnego nadzoru wspiera gospodarkę, pomaga trzymać z dala „osoby niepożądane”, daje pozór skutecznego działania, daje wrażenie, że „wszystkie wyjścia są zablokowane” oraz wspiera postawę „wszystko idzie jak zwykle”.

3. Definicja nadzoru, śledzenie społeczeństwa nadzorowanego

3.1. Definicje są ważne, szczególnie w przypadku tak kontrowersyjnego pojęcia jak nadzór. O nadzorze często myśli się stosując określone, charakterystyczne pojęcia, ale w istocie oznacza on znacznie więcej. Zamiast zaczynać od przedstawiania rozumienia nadzoru przez służby wywiadowcze czy służby policji, lepiej zacząć od szeregu zjawisk, które mają podobne cechy. Jeżeli mamy do czynienia z celowym, rutynowym, systematycznym i skonkretyzowanym zwracaniem uwagi na dane osobowe na potrzeby kontroli, nadawania uprawnień, zarządzania, wpływania lub ochrony, jest to nadzór.

3.2. Zbadajmy poszczególne elementy:

⁸ Zostało to omówione w: Lyon, D. (2003) *Surveillance after September 11 [Nadzór po 11 września]*, Cambridge UK: Polity Press, 45-48, 142 i nast.

- Zainteresowanie jest przede wszystkim *celowe*; obserwacja jest celowa, uzasadniona potrzebą kontroli, nadania uprawnienia lub innym oficjalnie zatwierdzonym celem.
 - Jest *rutynowe*; ma miejsce w momencie wykonywania przez nas codziennych czynności, jest elementem życia.
 - Jednak nadzór jest także *systematyczny*; jest zaplanowany i prowadzony zgodnie z planem, który jest ukierunkowany, a nie wyłącznie przypadkowy.
 - Jest wreszcie *skonkretyzowany*; nadzór wchodzi w szczegóły. O ile w pewnym stopniu nadzór opiera się na zagregowanych danych, znaczna jego część obejmuje osoby możliwe do zidentyfikowania, których dane są gromadzone, przechowywane, przekazywane, odzyskiwane, porównywane, poddawane analizie i sprzedawane.
- 3.3. Informacje te mogą być różne: zdjęcia z telewizji przemysłowej, informacje biometryczne takie jak odciski palców lub skany tęczówki, zapisy połączeń lub treści rozmów telefonicznych albo po prostu dane numeryczne lub kategoryczne. Z uwagi na to, że dużo danych dotyczących transakcji, wymiany, statusu, rachunków i tak dalej jest tego ostatniego rodzaju, Roger Clarke nazwał to „nadzorem danych” (*dataveillance*).⁹ Nadzór danych polega na monitorowaniu lub kontrolowaniu działania lub kontaktów ludzi w sposób zautomatyzowany, z wykorzystaniem technologii informacyjnych. Jest to o wiele tańsze niż bezpośredni lub specjalny elektroniczny nadzór i dlatego daje korzyści, które czasami mogą stanowić zachętę do rozszerzania systemu, nawet jeżeli dane nie są potrzebne do realizacji początkowo założonego celu.
- 3.4. Obecnie nadzór najczęściej ma opisaną wyżej formę, jednak nie można zapominać, że bezpośredni nadzór nad ludźmi istnieje nadal i jest prowadzony w ogromnej większości przez duże organizacje, które są zainteresowane realizacją jednego z wymienionych celów. Jednak koszty sprzętu do nadzoru zachęcają także innych do działań zautomatyzowanych, które obejmują patrzeć, obserwować, a nawet podpatrywanie i podglądanie. Pewien wzajemny nadzór ma miejsce, gdy małżonkowie korzystają z telefonów komórkowych w celu kontrolowania się (i znów mamy do czynienia z brakiem zaufania), a obserwacja oddolna może występować wtedy, gdy zwykli ludzie biorą aparat i obserwują obserwowanych.¹⁰
- 3.5. Co więc z nadzorem jako pojęciem opisującym rodzaj społeczeństwa? Skąd pochodzi idea społeczeństwa nadzorowanego? Zaczęła pojawiać się, co nie dziwi, po pierwszej fali komputeryzacji firm w latach 70. W tym czasie „Wielki Brat” ze słynnej powieści G. Orwella „Rok 1984” stał się kluczową metaforą. W latach 80. wiele poważnych analiz zaczęło zastępować te z lat 70.¹¹ i w niektórych z nich zaczęto stosować pojęcie „społeczeństwa nadzorowanego”. W 1985 r. Gary T. Marx odniósł się do „Roku 1984” w pierwszej naukowej wypowiedzi na temat „społeczeństwa nadzorowanego”, następnie Oscar Gandy, odnosząc się do pracy Maxa Webera przeniesionej do czasów technologii cyfrowych, użył sformułowania

⁹ Clarke, R. (2006[1997]) „Introduction to dataveillance and information privacy [Wstęp do nadzoru nad danymi i prywatności informacji]”, <http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV>

¹⁰ Mann, S., Nolan, M and Wellman, B. (2003) „Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments [Sousveillance – tworzenie i wykorzystanie przenośnych urządzeń liczących dla celów gromadzenia danych w otoczeniu poddanym nadzorowi]”, *Surveillance & Society* 1(3): 331-355.

¹¹ Np.: Rule, J. (1973) *Private Lives, Public Surveillance* [Życie prywatne, nadzór publiczny], London: Allen Lane. Pozycje najlepiej znane w latach 80. to zapewne: Burnham, D. (1983) *The Rise of the Computer State* [Rozrost państwa komputerowego], New York: Vintage Books; oraz Marx, G.T. (1988) *Undercover: Police Surveillance in America* [Pod osłoną – nadzór policyjny w Ameryce], Berkeley: University of California Press.

„biurokratyczna kontrola społeczna”, które miało ostrzegać przed „społeczeństwem nadzorowanym”¹²

- 3.6. Co interesujące, nasze postrzeganie nadzoru państwowego często jest kształtowane przez książki i filmy. Dobrym przykładem jest „Proces” (1914) Franza Kafki, w którym enigmatyczna postać Józefa K. (co stało się z nazwiskiem?) stawia czoła nieznanym oskarżycielom stawiającym niejasne zarzuty, albo „Rok 1984” (1948) George’a Orwella, który maluje przerażający obraz dokładnego, potępiającego nadzoru państwa, uosobianego przez groźną, przerażającą postać Wielkiego Brata. Podkreślają one kluczowe znaczenie informacji (lub jej braku w przypadku nadzorowanych) dla biurokratycznych rządów w dobie ciągłego zagrożenia totalitaryzmem.
- 3.7. Tym, czego ani Kafka ani Orwell nie mogli przewidzieć była komputeryzacja i szeroka informatyzacja administracji. W końcu krzemowy mikroprocesor powstał dopiero trzydzieści lat po „Roku 1984”. Od lat 70. komputery dokonały masowej ekspansji na obszarach, w których pojawił się nadzór i kontrola biurokratyczna. Rozterki związane z nadzorem zostały znakomicie przedstawione w „Rozmowie” (1974), jednak film ten mówi przede wszystkim o konwencjonalnych metodach nadzoru i podsłuchu. Nowsze filmy takie jak „System” (1995), „Wróg publiczny” (1998) i „Raport mniejszości” (2002) w sposób bardziej bezpośredni zajmują się nadzorem wykorzystującym technologie informacyjne. W przypadku filmów ważniejsze jest jednak efektywne wykorzystanie możliwości technologicznych niż rzeczywiste codzienne konsekwencje życia w społeczeństwach nadzorowanych.
- 3.8. Dlatego pomocny jest powrót do nauk społecznych. Niezależnie od zmian, które miały miejsce w środowisku przedsiębiorców i w środowisku rządowym od czasów Webera – komputeryzacja, tworzenie sieci, globalizacja a nawet „zarządzanie relacjami społecznymi” – leżące u ich podstaw zasady nie zmieniają się. Dlatego postrzeganie nowoczesnego świata nadzoru przez Webera jest tak wymowne. Postrzegał on ten nadzór, czyli przechowywanie szczegółowych zapisów, zestawianie informacji, ograniczanie dostępu dla określonych osób, nie jako mało istotne potwierdzenie „postępu”, ale jako potwierdzenie bardzo dwuznaczne. Przewidział, że w najgorszym wypadku skuteczny, ale bezduszny świat biurokratycznych organizacji stanie się „żelazną klatką”. Zwykli ludzie będą czuli się zamknięci w bezosobowym, obcym systemie. Wystarczy dodać do tego obojętność przesłuchujących Józefa K. lub nieprzewidywalność takiego bezlitosnego dyktatora jak Wielki Brat i jest przepis na represję.
- 3.9. Należy jednak wyjść poza perspektywę Webera, ponieważ dzisiejsze społeczeństwo nadzorowane jest nie tylko zaawansowane technologicznie, ale już dawno przekroczyło granice państwa i weszło do korporacji, komunikacji a nawet rozrywki (telewizyjny program rozrywkowy *Big Brother* pokazuje jak nadzór jest osławiany i staje się w nowy sposób obecny¹³). Nadzór jest nierozłączny z tym co nazywamy „kierowaniem”. Ma znacznie szerszy zakres niż działania rządów; „państwo komputerowe” jest już dziś przestarzałą ideą. Kierowanie odnosi się do różnych metod sterowania społeczeństwem i regulowania jego życia. Oznacza kontrolę dostępu, możliwości i szans a nawet pomaganie w dokonywaniu wyborów,

¹² Marx, G.T. (1985) „The surveillance society: the threat of 1984-style techniques [Społeczeństwo nadzoru – zagrożenie technikami z Roku 1984]” *The Futurist*, June: 21-26; Gandy, O. (1989) „The surveillance society: information technology and bureaucratic social control [Społeczeństwo nadzoru – technologia informacyjna i biurokratyczna kontrola społeczna]” *Journal of Communication*, 39:3.

¹³ Zob.: McGrath, J. (2004) *Loving Big Brother [Kochający Wielki Brat]*, London: Routledge; Andrejevic, M. (2004) *Reality TV: The Work of Watching [Reality TV – oglądanie jako praca]*, Lanham MD: Rowman and Littlefield.

często z wykorzystaniem danych osobowych w celu określenia, kto co dostaje. Praktyki urzędnicze zbyt często zastępują zasady etyczne.

4. Perspektywy dotyczące społeczeństwa nadzorowanego 1: problemy

4.1. Przechodzimy do zestawu problemów i procesów odnoszących się do społeczeństwa nadzorowanego, takiego które zostało opisane wyżej. Chodzi o stworzenie katalogu lub wykazu ważnych kwestii, które należy uwzględnić w dyskusji na temat społeczeństwa nadzorowanego. Należy zauważyć, że chociaż te kwestie zmieniają się w zależności od czasu i miejsca, w pewnym sensie mają ogromne znaczenie dla zrozumienia podstawowych cech społeczeństwa nadzorowanego.

4.2. Prywatność, etyka, prawa człowieka.

4.2.1. Lata 70. to czas poważnej refleksji i debaty prawnej na temat nadzoru, czego efektem były akty prawne o ochronie danych w Europie oraz akty prawne dotyczące ochrony prywatności poza nią. W przepisach tych przyjęto specyficzne rozumienie prywatności. Chociaż zasady bezpiecznego obrotu informacjami (*Fair Information Principles - FIP*)¹⁴, które ewoluowały i zostały powszechnie zaakceptowane wynikają ze zwykłego zrozumienia znaczenia prywatności dla jednostek, trudne okazało się przekonanie decydentów politycznych o znaczeniu *społecznego* wymiaru prywatności¹⁵, nie mówiąc o potrzebie skonfrontowania problemów związanych ze społeczeństwem nadzorowanym jako takim. Chodzi także o to, że aby podjąć procedurę prawną dana osoba musi wiedzieć, że coś jest nie tak, zorientować się to co jest i wiedzieć gdzie się z tym zwrócić i jakie podjąć działania.

4.2.2. Ze zjawiskiem społeczeństwa nadzorowanego wiążą się rozterki dotyczące etyki i praw człowieka, które wykraczają poza kwestię prywatności. Nie umniejszając ludzkiej i demokratycznej potrzeby prywatności i przyznając, że gdyby tylko duże organizacje w pełni przestrzegały prawa dotyczącego ochrony danych i prywatności, wiele problemów społeczeństwa nadzorowanego udałoby się zmniejszyć, uważamy, że te problemy powinny być analizowane w inny sposób. Nadzorowane osoby, chociaż poinformowane, nie powinny być zmuszane do chronienia samych siebie. Następujące problemy są kluczowe:

4.3. Wykluczenie społeczne, dyskryminacja.

4.3.1. Jak pokazujemy w niniejszym raporcie, intensywność nadzoru zmienia się w zależności od miejsca oraz klasy społecznej, pochodzenia etnicznego i płci. Nadzór, naruszanie prywatności i ochrona prywatności różnią się w poszczególnych grupach, co wiąże się z preferencyjnym traktowaniem jednych grup i dyskryminowaniem innych. Oczywiście nie z powodu nadzoru państwo dziś czuje, że nie może dłużej oferować takiego zabezpieczenia społecznego, do jakiego aspirowało lub że teraz ogranicza swoje cele do zapewniania tylko pewnych form podstawowego bezpieczeństwa.¹⁶ Nadzór raczej zwiększa się wraz z tymi zmianami i zazwyczaj je wspiera lub przynajmniej umożliwia ich wprowadzenie. Wspieranie bezpieczeństwa indywidualnego można łatwo powierzyć komuś z zewnątrz.

¹⁴ FIP to północnoamerykański odpowiednik europejskich „zasad ochrony danych.”

¹⁵ Zob. doskonałe omówienie społecznego wymiaru prywatności: Regan, P. (1995) *Legislating Privacy: Technology, Social Values, and Public Policy* [Prywatność w ustawodawstwie – technologie, wartości społeczne i polityka publiczna], Chapel Hill: University of North Carolina Press.

¹⁶ Zob. np.: omówienie w: Bauman, Z. (2006) *Liquid Fear* [Płynny strach], Cambridge UK: Polity Press.

4.3.2. Zdrowie i opieka od kołyski aż po grób, będące dumnymi hasłami socjaldemokratycznych rządów zostały zredukowane do zarządzania ryzykiem, a takie zarządzanie ryzykiem wymaga pełnego rozeznania w sytuacji – i to tu pojawia się społeczeństwo nadzorowane. Dane osobowe są więc potrzebne do tego, aby się zorientować, gdzie kierować zasoby.¹⁷ A z uwagi na to, że sieci nadzoru pozwalają na współpracę, towarzystwa ubezpieczeniowe mogą dużo łatwiej współpracować z policją, a supermarkety mogą łączyć siły z innymi podmiotami gromadzącymi dane. W rezultacie, jak zobaczymy, policja częściej interweniuje w dzielnicach zamieszkałych przez ludność inną niż biała, a supermarkety są usytuowane w lepszych dzielnicach z łatwym dostępem dla osób poruszających się samochodem.

4.4. *Wybór, władza i nadawanie uprawnień.*

4.4.1. Jaki wpływ na kształtowanie społeczeństwa nadzorowanego mają zwykli obywatele, konsumenci, pracownicy i podróżujący? Należy jeszcze raz podkreślić, że społeczeństwo nadzorowane nie jest spiskiem ani dziełem nowych technologii. Zwykli ludzie potrafią to rozróżnić – i rozróżniają – szczególnie kiedy zależy im na przestrzeganiu zasad i prawa, kiedy kwestionują lub odmawiają wykorzystywania ich danych do celów, o których nie mają wystarczających informacji lub co do których mają wątpliwości.

4.4.2. Ale do jakiego stopnia poszczególne osoby i grupy osób mogą decydować się na bycie nadzorowanymi oraz ograniczać gromadzenie i wykorzystywanie danych osobowych? Kiedy system nadzoru jest elementem infrastruktury i kiedy jego funkcjonowanie jest techniczną zagadką, bardzo trudno jest osiągnąć znaczną różnicę. Na przykład konsumenci dowiadują się, jaki jest zakres tworzenia profilu osobowego prowadzonego przez większość korporacji dopiero gdy wybucha skandal związany z kradzieżą tożsamości.¹⁸ Nawet wówczas mówi się raczej o zabezpieczeniu – jak unikać podobnych nadużyć – niż o ograniczaniu uprawnień korporacji i organów państwowych w przetwarzaniu tak dużej ilości danych. Chociaż, jak wyjaśniamy dalej, ludzie nie są pozostawieni sami sobie wobec regulowania nadzoru, który może w dużym stopniu zależeć od wyspecjalizowanych agencji i komisji w krajach, które dysponują uregulowaniami prawnymi dotyczącymi ochrony danych i prywatności oraz od innych stowarzyszeń, mechanizmy te niekoniecznie są skuteczne. Osoby prywatne są w bardzo niekorzystnej sytuacji jeżeli chodzi o skutki nadzoru.

4.5. *Przejrzystość, odpowiedzialność.*

4.5.1. Uprawnienia podmiotów handlowych, transportowych i rządowych szybko się zwiększają, ale osoby prywatne i grupy mają trudności z uzyskaniem informacji na temat tego, co dzieje się z ich danymi osobowymi, kto je przetwarza, kiedy i w jakim celu. W istocie zwykli obywatele i klienci najczęściej po prostu nie mają czasu ani ochoty na zdobywanie takich informacji. Jednak stopniowo ich dane osobowe są wykorzystywane do kształtowania ich życiowych szans i kierowania ich wyborami. Wobec uprawnień dużych organizacji, które dysponują dużymi możliwościami nadzoru, wydaje się jednak uczciwe, aby zwykli ludzie mieli coś do

¹⁷ Ericson, R. and Haggerty, K. (1997) *Policing the Risk Society [Strategie w społeczeństwie ryzyka]*, Toronto: University of Toronto Press.

¹⁸ Zob. Artykuł wstępny w *New York Times* „The data-fleecing of America [Ameryka pełna danych]” 21.6.2005.

powiedzenia nawet jeżeli chodzi tylko o zasadę. Można to osiągnąć nie tylko poprzez wyspecjalizowane agencje, ale także grupy samopomocy i środki masowego przekazu.

- 4.5.2. Organizacje powinny ponosić odpowiedzialność, szczególnie kiedy szeroki nadzór odbywa się w sposób regularny i może mieć potencjalnie szkodliwe konsekwencje. Chociaż nadzór w miejscu pracy może uwidaczniać pewne nadużycia, jak zobaczymy, co najmniej w kilku miejscach pracodawcy byli zobowiązani przez związek zawodowy do ograniczenia monitorowania. Jak pokazują przykłady, dużo można osiągnąć dzięki przejrzystemu procesowi wyjaśniania przez pracodawców, z czym wiąże się monitorowanie i negocjowania jego akceptacji przez pracowników. Jeżeli jednak chodzi o nadzorowanie konsumentów, nie ma podobnego przykładu, tymczasem działania Tesco czy Walmart związane z danymi odbywają się na nieporównywalną skalę. Pojawienie się dzisiejszego społeczeństwa nadzorowanego wymaga przejścia od samodzielnej ochrony prywatności do odpowiedzialności podmiotów dysponujących danymi. Praca taka jest równoległa z wysiłkami prawodawców na rzecz wzmocnienia kontroli i naciskami na minimalizowanie nadzoru.

5. Perspektywy dotyczące społeczeństwa nadzorowanego 2: procesy

5.1. *Klasyfikowanie społeczeństwa.*

- 5.1.1. W społeczeństwie nadzorowanym podział społeczeństwa na grupy jest powszechny. Instytucje rządowe i środowisko biznesu analizują dane osobowe, które dzielą na kategorie w celu określenia rynków docelowych i grup ryzyka.¹⁹ W sekcji dotyczącej nadzorowania konsumentów zobaczymy jak firmy takie jak *Amazon.com* używają skomplikowanych technik pozyskiwania danych w celu określania profilu konsumentów z zastosowaniem oczywistych i nieoczywistych powiązań między danymi. Umożliwia im to określenie kto i co kupi najchętniej, ale także którzy konsumenci należą do grupy ryzyka. W przypadku *Amazon.com* ty jesteś ich profilem. *Amazon.com* czerpie z tego korzyści i z pewnością niektórzy konsumenci również. Otrzymywanie ofert umożliwia oszczędzanie czasu, który poświęciłoby się na wyszukiwanie. Konsekwencje dla konsumentów mogą także być niekorzystne. Po klasyfikacji trudno jest wyjść z danej kategorii. Takie nieoczywiste powiązania są także potrzebne przy klasyfikowaniu grup, które chcą podróżować samolotem. Po 11 września 2001 r. klasyfikowanie mogło przyczynić się do bezpieczeństwa w powietrzu (czy na pewno, nigdy się nie dowiemy), ale z pewnością doprowadziło do tworzenia profili grup, szczególnie muzułmanów, co spowodowało trudności, niedogodności, a nawet cierpienie.

- 5.1.2. Klasyfikowanie społeczeństwa w coraz większym stopniu definiuje społeczeństwo nadzorowane. Daje różne możliwości różnym grupom i często sprowadza się do nieznacznego a czasami niezamierzonego kierowania społeczeństwami oraz podejmowania decyzji bez demokratycznej debaty. Jak pokazano w części poświęconej infrastrukturze miejskiej, niewidoczne, przyjmowane jako oczywiste systemy pobierania opłat za przejazd i transport publiczny dzielą miasto na grupy, które mogą podróżować swobodnie i grupy, dla których podróżowanie jest utrudnione a jednocześnie może być wykorzystywane do zwalczania przestępczości i zapewniania bezpieczeństwa

¹⁹ Zob. klasyczne opracowanie: Gandy, O. (1993) *The Panoptic Sort: A Political Economy of Personal Information* [Sortowanie panoptyczne – polityczna ekonomia informacji osobowych], Boulder CO: Westview Press.

narodowego. Nikt nie opowiadał się za takimi systemami. Pojawiły się one w związku ze wspólnym rządzeniem, obsługą zewnętrzną, presją korporacji technologicznych i wzrostem działalności ubezpieczeniowej.

5.2. Przepływ danych.

5.2.1. Dane gromadzone przy pomocy technologii nadzoru przepływają w sieciach komputerowych. Wiele osób wyraża zgodę na przetwarzanie danych w jednej sytuacji, ale co się stanie, gdy te dane zostaną następnie przekazywane gdzie indziej? W celu ochrony dzieci przed nadużyciami lub zwalczania oszustw w instytucjach publicznych coraz częściej sięga się do coraz bardziej zróżnicowanych baz danych. Jednak organy państwowe lub agencje wymiany danych posiadają zbyt małą wiedzę na temat tego, gdzie dokładnie dane są przekazywane. Idea polityki „opartej na informacji” przy dzisiejszych możliwościach urządzeń cyfrowych w zakresie tworzenia sieci i łączenia danych oznacza, że nadzór zaczyna funkcjonować na zasadzie własnej logiki.

5.2.2. Ale ta logika musi zostać poddana w wątpliwość, zbadana i sprawdzona szczególnie pod kątem procesów, które obejmują przepływ danych z jednego miejsca do drugiego. Takie przepływy danych wymagają opisu i analizy. Ważnym pytaniem jest – w jaki sposób bazy danych są zabezpieczane przed niedozwolonym dostępem lub wypływem danych? Jeszcze ważniejsze – w jakim zakresie dane powinny być przekazywane z jednego miejsca do innego? Jest to podstawowa kwestia FIP, która stała się teraz pilna, ponieważ zintegrowanie i ujednolicenie systemów opartych na informacji wydaje się słuszne zarówno pod względem technologicznym jak i administracyjnym.

5.3. Niezamierzona zmiana celu

5.3.1. Trzeci podkreślony tu proces został wspomniany już we wstępie. Dane osobowe gromadzone i wykorzystywane do jednego celu i dla spełnienia jednej funkcji często są wykorzystywane do innych celów i funkcji, które rozszerzają i intensyfikują nadzór i naruszanie prywatności poza to, co początkowo jest rozumiane i traktowane jako akceptowalne społecznie, etycznie i prawnie. W przypadku *Oyster cards* w Zjednoczonym Królestwie dane, które początkowo są wykorzystywane do sprzedaży usług transportu publicznego są coraz częściej wykorzystywane w śledztwach policyjnych.²⁰ Takie dane mogą także pozostać w tym samym obszarze, ale jeżeli ich wykorzystanie zwiększa się, mogą nabrać niebezpiecznych cech. Nadzór medyczny, jak zobaczymy, jest trafnym przykładem. Technologie diagnostyczne, które w poszczególnych przypadkach mogą być w pewnym stopniu przydatne, mogą rozrastać się na kolejne obszary, co zmniejsza ich użyteczność dla postawienia prawidłowej diagnozy. Osoby nieprawidłowo zdiagnozowane mogą znaleźć się w niekorzystnej sytuacji.

5.3.2. Zmiana celu zazwyczaj odbywa się po cichu, bez przeszkód, jako usprawnianie administracji. Stanowi jednak zagrożenie dla FIP i mimo tego, że określono je jako problem kilkadziesiąt lat temu, problem pozostaje aktualny. Z uwagi na to, że nowe technologie pozwalają na zwiększanie ilości wymienianych danych oraz że skuteczność organizacyjna jest często traktowana jako priorytet, konsekwencje zmiany celu są zbyt często nieznane lub bagatelizowane.

²⁰ Zob.: „Oyster data use rises in crime clamp-down [Wykorzystanie danych *Oyster* ujawnione w działaniach przeciwko przestępności]” *The Guardian*, 13 March 2006, <http://politics.guardian.co.uk/foi/story/0,,1730771,00.html>

5.4. Technologie.

5.4.1. Dziś o nadzorze często myśli się w sposób technologiczny. Technologie są bardzo ważne, ale należy także pamiętać o dwóch ważnych rzeczach: Jedną z nich jest bezpośredni „nadzór nad ludźmi” bez użycia technologii, który wciąż pojawia się i często wiąże się z nadzorem technologicznym. Po drugie, same systemy technologiczne nie są ani przyczyną ani sumą tego, czym nadzór jest dziś. Nie możemy po prostu rozpoznać konsekwencji nadzoru na podstawie możliwości każdego nowego systemu (szczególnie jeżeli te możliwości są opisane przez sprzedawcę). Ale jeżeli technologie są rzeczywiście ważne dla nadzoru, jak należy je postrzegać?

5.4.2. Aby zrozumieć społeczeństwo nadzorowane, należy stale analizować i monitorować nowe technologie. Musimy zrozumieć, jak one funkcjonują (jak działa sprzęt i oprogramowanie), jak są wykorzystywane (jest to proces interaktywny, angażujący personel wewnętrzny oraz konsultantów do spraw technologii i operatorów) i jak wpływają na funkcjonowanie organizacji. Co więcej, należy rozumieć te rzeczy wystarczająco jasno, aby wpływać na politykę i praktykę, co sugerujemy w dalszym omówieniu oceny wpływu.

5.4.3. Podobne technologie są dziś wykorzystywane w różnych miejscach, co sprzyja rozwojowi łączonego nadzoru. Ostatnie zjawiska, takie jak technologie lokalizacji, pozwalają na śledzenie osób i towarów w czasie rzeczywistym, a obecne zjawiska jak inteligentne środowisko wykorzystujące wbudowywane, noszone na sobie i wszczepiane urządzenia idą jeszcze dalej. Jedną ważną konsekwencją jest to, że osoby potrafiące dokonać krytycznej analizy społeczeństwa nadzorowanego pod względem etycznym powinny być zaangażowane na każdym etapie wdrażania. Systemy stają się dużo mniej podatne na zmianę po ich utworzeniu.

5.4.4. Trzecim problemem dotyczącym technologii jest to, że wiele osób uważa (jak zobaczymy, niesłusznie), że obawy związane ze społeczeństwem nadzorowanym można rozwiązać za pomocą rozwiązań technicznych. Z pewnością pewne tak zwane technologie podnoszące poziom ochrony prywatności (*privacy-enhancing Technologies* – PET) rzeczywiście służą do ograniczania rozwoju nadzoru technologicznego i ich wykorzystywanie powinno być w odpowiednich przypadkach promowane. Ale jest to tylko częściowa odpowiedź. Należy słusznie obawiać się naprawiania problemów technicznych za pomocą rozwiązań technicznych. Jak zobaczymy, prawdziwy świat społeczeństwa nadzorowanego jest za bardzo złożony na takie powierzchowne działania.

6. Przewodnik po raporcie.

6.1. Po wstępie (Część A) następuje kilka kolejnych części raportu:

- Część B przedstawia zawartość dziewięciu oddzielnych raportów ekspertów specjalnie zamówionych na potrzeby szerokiego badania społeczeństwa nadzorowanego.
- Część C ilustruje społeczeństwo nadzorowane, za pomocą historii przedstawiającej tydzień z życia fikcyjnej rodziny w 2006 r. oraz poprzez pokazanie, jak pewne spotkania i doświadczenia tej rodziny mogą wyglądać po dziesięciu latach, w roku 2016.

- Część D dotyczy tego, co decydenci (rząd i inne organy, takie jak rzecznik de. informacji) mogą zrobić w celu ograniczenia najgorszych aspektów nadzoru.
 - Część E zawiera sugestie dotyczące zapoznania się z kolejnymi dokumentami.
 - Wszystkie raporty ekspertów znajdują się w załącznikach.
- 6.2. Do pełnego raportu dołączono dokument do dyskusji publicznej, którego celem jest wywołanie dyskusji i debaty wśród opinii publicznej.

Część B

Badanie

społeczeństwa nadzorowanego

7. Wprowadzenie

- 7.1. Surveillance Studies Network [Sieć Studiów nad Nadzorem] zleciła sporządzenie szeregu specjalistycznych raportów, których teksty znajdują się w załączeniu. Raporty te dotyczą następujących zagadnień: zdrowie i medycyna, konsumpcja, praca i zatrudnienie, służby publiczne, obywatelstwo, przestępczość i wymiar sprawiedliwości, komunikacja, budownictwo i infrastruktura oraz granice. W raportach tych pojawiło się kilka kluczowych tematów, które można przyporządkować do czterech obszarów: kontekst społeczeństwa nadzorowanego; technologie nadzoru; procesy, dzięki którym funkcjonuje i jest wdrażany nadzór oraz wpływ nadzoru na poszczególne osoby i grupy w społeczeństwie. Obszary te oczywiście w dużej mierze pokrywają się; wiele zagadnień pozostaje również poza ich zasięgiem.

8. Kontekst społeczeństwa nadzorowanego

- 8.1. W pierwszym rzędzie opisujemy kilka obserwowanych w społeczeństwach zachodnich podstawowych tendencji, które prowadzą do powstania społeczeństwa nadzorowanego. Są to: zagrożenia i bezpieczeństwo; rola wojska; polityczne koszty nadzoru; wzrost roli informacji o danych osobowych.

8.2. Zagrożenie i bezpieczeństwo

- 8.2.1. Żyjemy w społeczeństwie, w którym panuje obsesja zagrożenia. Techniki zarządzania ryzykiem dotyczące zagrożeń zewnętrznych stały się kluczowym elementem działań organizacyjnych, które nasiliły się wraz z początkiem „wojny z terroryzmem”. Coraz częściej spotykamy również procedury oceny ryzyka wewnętrznego. Oczywiście zarządzanie ryzykiem po 11 września 2001 r. nie jest dziedziną całkowicie nową; istnieje bogate materiały historyczne dotyczące profilowania ryzyka przed 9/11.²¹

²¹ Bigo, D. (2002) „Security and immigration: toward a critique of the governmentality of unease [Bezpieczeństwo i imigracja: przyczynki do krytyki zarządzania w warunkach niepokoju]”, w: *Alternatives* (27): s. 63-92; Andreas, P., Snyder, T. (wyd.) (2000) „*The Wall Around the West: State Borders and Immigration Controls in North America and Europe* [Mur wokół Zachodu: kontrola granic państwowych i imigracji w Ameryce Północnej i Europie]”, Lanham MD: Rowman i Littlefield.

- 8.2.2. Pojawiło się jednak wyprzedzające podejście w stosunku do zagrożeń, w odróżnieniu od podejścia prewencyjnego.²² Stosowane obecnie i pojawiające się nowe praktyki obejmują w związku z tym technologie i pozyskiwanie danych. Charakterystyczne jest, że w ramach wyprzedzającego profilowania zagrożenia praktyki nadzoru przesuwają się w stronę klasyfikowania działań i transakcji prowadzonych przez całą populację.²³ Klasyfikacja taka może zostać następnie użyta w celu ukierunkowania interwencji na ludzi lub grupy osób, które uznaje się za zagrożone lub za stwarzające zagrożenie dla innych. Dlatego ważne jest też zbieranie i analiza informacji, w tym danych dotyczących osób dających się zidentyfikować.
- 8.2.3. Nadzór stanowi kluczowy element życia w warunkach zagrożenia do tego stopnia, że za bardziej właściwe można by uznać nazwanie społeczeństwa nadzorowanego „społeczeństwem nadzorującym zagrożenia”. Odpowiedzią na istnienie zagrożeń jest położenie nacisku na bezpieczeństwo. „Społeczeństwo nadzorujące zagrożenia” umożliwiło pojawienie się „państwa bezpiecznego”, ogarniętego obsesją bezpieczeństwa i stabilności. Motto towarzyszące wyraźnemu wzrostowi liczby przedstawianych do rozpatrzenia przez opiekę społeczną przypadków znęcania się nad dziećmi brzmi: „lepiej dmuchać na zimne”. Stwarza ono możliwość prowadzenia zapobiegawczego nadzoru służb publicznych nad pewnymi grupami, kategoriami i osobami. Takie podejście może wiązać się z korzyściami osobistymi i społecznymi, ale jednocześnie ta koncepcja bezpieczeństwa w znaczący sposób wpływa na wolność, kwestię prywatności i inne wartości społeczne, jak również na innowacje i zmiany, z czym nierozzerwalnie wiąże się ryzyko.
- 8.2.4. Taką tendencję do oceny ryzyka i profilaktyki zilustrować może kilka przykładów: pierwszy z nich dotyczy wzrostu udziału badań epidemiologicznych i modelowania w nadzorze medycznym²⁴. Nadzór medyczny dla celów zdrowia publicznego przybiera trzy główne postaci – w pierwszym rzędzie jest to monitoring i śledzenie poszczególnych przypadków chorób. Praktyka ta stosowana jest nie tylko z uwagi na ryzyko osobiste pacjenta, ale również w celu dokonania identyfikacji źródeł zakażenia i/lub ryzyka genetycznego, lokalizacji i ostrzeżenia potencjalnie zakażonych osób, które miały kontakt z osobą będącą nosicielem choroby zakaźnej (takiej jak AIDS lub gruźlica) lub dotkniętych chorobą krewnych, obciążonych takim samym ryzykiem genetycznym (np.: płaswicą Huntingtona). Po drugie, rejestracja zachorowań dla celów analizy statystycznej (np. rozpoznawanie zagęszczeń przypadków występowania raka poprzez analizę danych w rejestrze zachorowań na raka). Po trzecie, masowe badania całych populacji w celu wyróżnienia osób lub grup z wyższym niż średnie ryzykiem zachorowania (np. masowe badania ciśnienia krwi lub rutynowe badania mammograficzne w celu wczesnego wykrycia raka piersi). Debata w sprawie genetyki jest bardzo intensywna. Coraz częściej tworzone są coraz większe bazy danych zawierające informacje genetyczne dla służby zdrowia, wymiaru sprawiedliwości oraz dla celów komercyjnych.

²² Ewald, F. (2002) „The return of Descartes' malicious demon: an outline of a philosophy of precaution [Powrót złośliwego demona Descartes'a: zarys filozofii ostrożności]”, w: Baker, T. i Simon, J. (wyd.); *Embracing Risk: The Changing Culture of Insurance and Responsibility* [Kłopotliwe ryzyko: Zmieniająca się kultura ubezpieczeń i odpowiedzialności], Chicago: University of Chicago Press.

²³ Valverde, M., Mopas, M. (2004) „Insecurity and the Dream of Targeted Governance [Brak bezpieczeństwa i marzenie o ukierunkowanych rządach]”, w: Larner, W. i Walters, W. (wyd.) *Global Governmentality: Governing International Spaces*, London: Routledge.

²⁴ Ekonomia zdrowia zyskuje na znaczeniu. W dziedzinie tej szeroko stosowane są techniki i wyniki badań z zakresu specjalności od epidemiologii do oceny technologii medycznych, patrz np.: Ashmore, M., Mulkay, M.J. i Pinch, T.J. (1989) *Health and Efficiency: A Sociology of Health Economics* [Zdrowie i wydajność: Socjologia ekonomii zdrowia], Buckingham: Open University Press.

8.2.5. Po drugie, można zaobserwować szeroką gamę dziedzin polityki publicznej.²⁵ Metody oparte na ryzyku, opracowane w oparciu o oceny poszczególnych osób, rodzin i wspólnot sąsiedzkich stosowane są w dziedzinie ochrony dzieci i zdrowia psychicznego, jak również w dziedzinie wymiaru sprawiedliwości w ramach ochrony publicznej. Statystyki dotyczące wspólnot sąsiedzkich zostały stworzone w związku z potrzebą posiadania lepszej jakości danych na potrzeby dostosowanych i ukierunkowanych interwencji, prowadzonych ze wsparciem metod wywiadowczych, koordynowanych przez kilka instytucji.²⁶ Niektóre podstawowe programy, takie jak na przykład program dla dzieci SureStart, intensywnie wykorzystują dane dotyczące poszczególnych osób. Statystyki służą również do wspierania wysiłków mających na celu zwalczanie wykluczenia społecznego oraz, w szczególności, interwencje w sektorze edukacji, a także wdrażanie nowych inicjatyw, takich jak bazy danych dotyczących dzieci.

8.2.6. W wymiarze sprawiedliwości zagrożenie stało się głównym elementem, a wspieranie obecnego celu strategii stosowanych przez policję i Ministerstwo Spraw Wewnętrznych (Home Office) wiąże się z trwałym zobowiązaniem do wykorzystywania strategii i technologii nadzoru w działaniach mających na celu nie tylko ogólne zmniejszenie przestępczości, ale też, w szczególności, identyfikację osób zagrożonych przestępczością, proaktywne skupienie się na grupie notorycznych przestępców, którzy zdaniem władz są w największym stopniu odpowiedzialni za problem przestępczości²⁷.

8.2.7. Ocena ryzyka stała się decydującym kryterium nadzoru granicznego – od ochrony granic państwa do pilnowania transgranicznych przepływów finansowych, od bezpieczeństwa portów lotniczych do prześwietlania kontenerów w portach morskich. Współczesny nadzór graniczny obejmuje kompilację, klasyfikację i podział na kategorie danych dotyczących na przykład list pasażerów lub transakcji finansowych, prowadzone na niespotykaną dotychczas skalę. System kontroli granicznej USVISIT²⁸ dla obywateli Wielkiej Brytanii przekraczających granicę USA przeszukuje około 30 baz danych, zawierających dane dotyczące wjazdu i wyjazdu, informacje dotyczące ubezpieczeń społecznych i wymiany studentów.

8.2.8. Wykorzystywanie w ocenie ryzyka szczegółowych informacji o danych osobowych oraz medycznych leży zarówno w interesie pracodawców, jak i branży usług finansowych. Chociaż obecnie praktyka ta nie jest stosowana, możliwość zastosowania połączenia informacji konsumenckich i medycznych

²⁵ .6, P., Raab, C. i Bellamy, C. (2005) „Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I [Połączenie rządów i prywatności w Zjednoczonym Królestwie: Zarządzanie napięciami pomiędzy ochroną danych i polityką społeczną, Część I]”. *Public Administration* 83 (1): s. 111-133; „Joined-up government and privacy in the United Kingdom: Managing tensions between data protection and social policy, Part I [Połączenie rządów i prywatności w Zjednoczonym Królestwie: Zarządzanie napięciami pomiędzy ochroną danych i polityką społeczną, Część II]” *Public Administration* 83 (2): s. 393-415.

²⁶ Social Exclusion Unit, Cabinet Office [Jednostka ds. Wykluczenia Społecznego, Urząd Rady Ministrów] (2000) „*Report of Policy Action Team 18 on Better Information* [Raport 18 zespołu operacyjnego Policji w sprawie lepszej jakości informacji]”. London: Social Exclusion Unit, Cabinet Office; Department for Work and Pensions [Ministerstwo Pracy i Emerytur] (2001) „*United Kingdom National Action Plan on Social Exclusion 2001-03* [Brytyjski Narodowy Plan Działań w zakresie Wykluczenia Społecznego 2001 - 2003]”. London: Department for Work and Pensions.

²⁷ Home Office [Ministerstwo Spraw Wewnętrznych] (2001a) „*Criminal Justice: The Way Ahead* [Prawo karne: droga postępu]”, Cm 5074, London: Home Office, 20-23; aby zapoznać się z krytyczną opinią na temat tej polityki patrz: Garside, R. (2004) „*Crime, Persistent Offenders and the Justice Gap* [Przestępczość, recydywiści i luka w wymiarze sprawiedliwości]”, London: Crime and Society Foundation.

²⁸ Technologia wskaźników dotyczących statusu gościa i imigranta w Stanach Zjednoczonych (United States Visitor and Immigrant Status Indicator Technology), stosowana począwszy od 2004 r. na wszystkich lądowych, powietrznych i morskich przejściach granicznych.

do celów sprawdzania wiarygodności kredytowej oraz dla celów ubezpieczeniowych budzi poważne obawy dotyczące dokładności danych, wykorzystania danych i oszustw. Zwiększenie zarówno ilości, jak i jakości tych danych stanowi wprawdzie metodę likwidacji tych zagrożeń ale takie rozwiązanie samo w sobie może wiązać się z nieprzyjemnymi konsekwencjami. W zależności od sposobu wykorzystania informacji, szanse życiowe i możliwości osób korzystających ze służb specjalnych i/lub polegających w znacznym stopniu na ich pomocy mogą zostać w znacznym stopniu ograniczone, ponieważ osoby takie mogą zostać określone jako „osoby wysokiego ryzyka”. Odnosi się to również do całych populacji zamieszkujących pewne obszary. Przy wykorzystaniu danych geodemograficznych można dokonać identyfikacji całych ulic, kodów pocztowych lub nawet większych obszarów i przypisać im właściwy poziom zagrożenia. W takim przypadku ryzyko inwestycyjne przeniesione zostaje z danej organizacji na jej potencjalnych klientów lub użytkowników (oraz ich lokalizację geograficzną), pomimo że istnieje niewiele oznak, które mogłyby wskazywać na wzrost lub spadek ryzyka kosztowego.

- 8.2.9. Dane osobowe, medyczne oraz dane biometryczne postrzegane są obecnie przez pracodawców jako sposób potwierdzenia tożsamości pracowników oraz metoda zarządzania zdrowiem i bezpieczeństwem. Na przykład, po szerokim zastosowaniu w USA kontroli spożycia alkoholu i zażywania narkotyków w pracy, praktyka ta stosowana jest coraz częściej w Wielkiej Brytanii, zwłaszcza w odniesieniu do pracy w niebezpiecznych warunkach (np. prowadzenie pojazdów).

8.3. *Militaryzacja nadzoru*

- 8.3.1. Dążenie do bezpieczeństwa przynajmniej częściowo stanowi dowód na to, że wojsko w dalszym ciągu ma znaczenie dla zachodnich społeczeństw lub też, że znaczenie to zostało ponownie odbudowane. Nadzór wojskowy jest jednym z niewielu zjawisk, o których można powiedzieć, że mają charakter prawdziwie globalny w epoce, w której teoretycznie wszystko ulega globalizacji. Sieć krążących wokół Ziemi satelitów nadzoru wojskowego staje się coraz gęstsza.

- 8.3.2. Ponadto międzynarodowe systemy komunikacyjne są wnikliwie analizowane i infiltrowane przez wojskowe systemy nadzoru: nawet ich wynalezienie, stosowane w nich protokoły oraz sposób, w jaki są skonstruowane, zawierają elementy wojskowe. Jednym z przykładów jest Globalny System Pozycjonowania (GPS – Global Positioning System), który został opracowany i wciąż znajduje się pod ostateczną kontrolą amerykańskich władz wojskowych. Mogą one zmienić jego cechy użytkowe w określonych miejscach i w określonym czasie, jeżeli odpowiada to celom wojskowym. Kolejnym przykładem jest Internet. Ten międzynarodowy system połączeń sieciowych i protokołów powstał całkowicie w oparciu o ARPANET, amerykański wojskowy rozproszony system komunikacji, opracowany tak, aby mógł funkcjonować pomimo zniszczenia poszczególnych części systemu²⁹. Tak naprawdę całą historię nowoczesnego nadzoru można prześledzić od wczesnych faz rozwoju, którego korzeni szukać należy w systemach łączności z czasów drugiej wojny światowej i zimnej wojny, takich jak system łączności, kontroli i wywiadu *Command Communications, Control and Intelligence* (C3I), których

²⁹ Rheingold, H. (1994) „*The Virtual Community* [Społeczność wirtualna]”, London: Secker and Warburg.

celem było uczynienie z Ziemi „zamkniętego świata” – całkowicie bezpiecznej i możliwej do obrony przestrzeni³⁰.

8.3.3. Rozwój technologii i procedur nadzoru wynika ze złożonego współoddziaływania logiki wojskowej i gospodarczej. Wojskowe sposoby organizacji i metody kontroli zawsze były głównym elementem rozwoju nowoczesnego świata. To właśnie kontrola zasobów wojskowych i uprawnienia do użycia siły przysługujące instytucjom państwowym leżą u podstaw nowoczesnych państw narodowych. To współoddziaływanie przejawia się nie tylko w administracji i technologii, ale także w coraz bardziej wojskowym sposobie mówienia o codziennym bezpieczeństwie: czynniki państwowe i środki masowego przekazu mówią o „ocenie zagrożenia”, „wojnie z narkotykami”, „wojnie z przestępczością” i wreszcie o „wojnie z terroryzmem”, o bezwzględny stosowaniu prawa, o „strategii zero tolerancji” itd. Pojęcia obronności i bramkowania (zamykanie określonych obszarów) stały się kluczowymi elementami planowania urbanistycznego. „Wojna informatyczna” miała swój początek w mrokach tajnych operacji i ujrzała światło dzienne w świecie biznesu, gdzie powszechne jest szpiegostwo gospodarcze, a specjaliści od przeszukiwania zawartości komputerów i tworzenia zabezpieczeń określani są mianem „wojowników wiedzy”.

8.3.4. Jeżeli jednak przyjrzyć się historii różnych technologii, można znaleźć wiele konkretnych przykładów: wiele firm zajmujących się technologiami nadzoru posiada potajemne związki z instytucjami wojskowymi, pomimo faktu, że firmy te sprzedają swoje produkty coraz większej liczbie użytkowników cywilnych. Istnieją dowody, że firmy zaopatrujące wojsko i produkujące broń przerzucają się na rynki cywilne oraz że tworzą się nowe rynki innowacyjnych produktów. Rynki te nie mają już charakteru czysto wojskowego lub czysto cywilnego³¹. Główni producenci broni zmieniają profil, przechodząc do produktów z zakresu bezpieczeństwa i nadzoru: dobry przykład stanowi rozwój firmy TRW, jednego z głównych zleceńbiorców USA w zakresie obronności, która stała się liderem w dziedzinie cywilnej biometryki. W Wielkiej Brytanii taki przykład stanowi częściowo sprywatyzowana firma QinetiQ, która dawniej nosiła nazwę Defence Evaluation and Research Agency [DERA – Agencja oceny i badań w dziedzinie obronności] a we Francji – Sagem. Wytwarzają one obecnie bardzo szeroką gamę produktów – od telefonów komórkowych poprzez algorytmy nadzoru do bezzałogowych systemów powietrznego rozpoznania.

8.3.5. W latach dziewięćdziesiątych XX wieku wielu specjalistów dowodziło, że przechodzenie producentów broni na produkcję cywilną jest tendencją pozytywną, częścią „pokoju dywidendy” czasów po zakończeniu zimnej wojny i dobrym społecznym, które najprawdopodobniej ma swoje źródło w upadku Związku Radzieckiego. Jednakże ci producenci, którzy wcześniej specjalizowali się w dostawach dla wojska, zajęli się produkcją cywilną bez odcinania się od swoich wojskowych „korzeni”. Wraz z początkiem „wojny z terroryzmem” powrót tych producentów do produkcji dla celów wojskowych

³⁰ de Landa, M. (1991) „*War in the Age of Intelligent Machines* [Wojna w epoce inteligentnych maszyn]”, Cambridge MA: MIT Press; Edwards, P. (1997) „*Computers and the Politics of Discourse in Cold War America* [Komputery i polityka rozmów w Ameryce czasów zimnej wojny]”, Cambridge MA: MIT Press.

³¹ Wright, S. (1998) „*An Appraisal of the Technologies of Political Control: Interim STOA Report (PE 166.499)* [Ocena technologii kontroli politycznej: Raport śródkresowy STOA (PE 166.499)]”, Luksemburg: Parlament Europejski, Dyrekcja Generalna ds. Badań, Dyrekcja A, Program STOA; Doucet, I. i R. Lloyd (wyd.) (2001) „*Alternative Anti-Personnel Mines: The Next Generation* [Alternatywne miny przeciwpiechotne: Następna generacja]”, London / Berlin: Landmine Action / German Initiative to Ban Landmines [Akcja w sprawie min przeciwpiechotnych/ Niemiecka inicjatywa na rzecz wprowadzenia zakazu stosowania min przeciwpiechotnych].

był nader szybki; podobnie było z wieloma nowymi firmami zajmującymi się dziedziną bezpieczeństwa, specjalizującymi się w różnych technologiach nadzoru.

8.4. *Polityczne koszty nadzoru*

8.4.1. Nowe firmy, o których była mowa powyżej, wraz z tradycyjnymi instytucjami strzegącymi bezpieczeństwa i dużymi dostawcami materiałów wojskowych tworzą część tego, co ogólnie można określić mianem „branży bezpieczeństwa”. Inne sektory przemysłu również są elementami kluczowymi dla rozwoju nadzoru, a w szczególności nadzoru systemów telekomunikacyjnych, informatycznych, nadzoru bankowego i ubezpieczeniowego.

8.4.2. W ostatnich latach branża bezpieczeństwa bardzo wyraźnie się rozrosła. Istnieją liczne sposoby zmierzenia tego wzrostu. Na przykład amerykański konsultingowy skorowidz firm Security Stock Watch 100 wymienia w branży bezpieczeństwa następujące specjalności: „obrona biologiczna”, „bezpieczeństwo środowiska”, „zapobieganie oszustwom”, „obrona wojskowa”, „bezpieczeństwo sieci” telekomunikacyjnych oraz „ochrona fizyczna” (bariery, nadzór kamer wideo itp.). Zgodnie z tym skorowidzem rozwój całej tej branży stale przewyższa wskaźniki zarówno indeksu Dow Jones, jak i indeksu zaawansowanych technologii NASDAQ³². Pod koniec roku finansowego 2005-2006 skorowidz ten zwiększył swoją objętość ponad dwukrotnie, przy czym szacowana kapitalizacja rynkowa dla 100 ujętych w skorowidzu firm wyniosła ponad 400 miliardów dolarów. Mając na uwadze rozmiary i liczbę innych firm w tym sektorze na całym świecie, kwota ta może być według ostrożnych szacunków dwa razy większa.

8.5. *Gospodarowanie informacjami o danych osobowych*

8.5.1. Nadzór prowadzą nie tylko państwa i organizacje, ale także zwykli ludzie. Po zamachach bombowych w Londynie w 2005 roku zarówno sieci telewizyjne, jak i policja zachęcały ludzi do fotografowania podejrzanych osobników przy pomocy aparatów fotograficznych wbudowanych w telefony komórkowe. Coraz więcej ludzi, szczególnie dzieci i młodzieży wystawia na pokaz swoje życie, obserwując w zamian, jak żyją inni, za pośrednictwem funkcjonujących w czasie rzeczywistym kamer internetowych³³ oraz takich stron jak *MySpace* czy *Bebo*.

8.5.2. Jednocześnie osoby posiadające szerszy dostęp do zasobów wiedzy dochodzą do wniosku, że warto jest podejmować próby śledzenia „podwójnych danych”, powstających w wyniku stosowania różnych form nadzoru, któremu podlegamy. Działanie takie zaczęło mieć zasadnicze znaczenie dla szans życiowych, zwłaszcza w związku z faktem, że określanie zdolności kredytowej i inne rodzaje rankingów wartości osób, tworzone z wykorzystaniem baz danych, stają się podstawą świadczenia całej gamy usług. Agencje badające zdolność kredytową oferują na bieżąco dostęp do rejestrów zdolności kredytowej osób prywatnych, umożliwiając podważenie i poprawienie

³² *SecurityStockWatch.com 100 Index*, sierpień 2006 r., <http://www.securitystockwatch.com/>

³³ Koskela, H. (2004) „Webcams, TV Shows and Mobile phones: Empowering Exhibitionism [Kamery internetowe, programy telewizyjne i telefony komórkowe: Upelnomocnienie ekshibicjonizmu]”, *Surveillance & Society*, CCTV Special (wyd.: Norris, McCahill i Wood), 2(2/3): s. 199-215, <http://www.surveillance-and-society.org/cctv.htm>

mylących danych. Takie połączenie dobrowolnej otwartości firm i działalności samouków nie może być wiarygodne jako forma regulacji, tym niemniej nowe pokolenie młodych ludzi może dojrzywać jako obywatele przyzwyczajeni do prowadzenia nadzoru, bycia jego przedmiotem i obcowania z nim.

9. Technologie nadzoru

9.1. W naszym badaniu technologii nadzoru, zanim postawimy pierwsze, ogólne tezy dotyczące rozwoju i rozpowszechniania technologii nadzoru, w pierwszym rzędzie planujemy rozważyć zasadnicze znaczenie zwykłego nadzoru, niebędącego nadzorem technologicznym. Następnie skupimy się na powiązanych ze sobą i zazębiających się kierunkach postępu w czterech obszarach technologicznych: telekomunikacji, utrwalaniu obrazów i dźwięków, cyfrowych technologii informatycznych oraz w technologii wykorzystującej znaczniki i systemy namierzania. Przeanalizujemy również wzajemne powiązania pomiędzy różnymi technologiami oraz tendencję do wprowadzania niewidocznych, a jednocześnie wszechobecnych technologii nadzoru. Opracowanie niniejsze zakończymy omówieniem granic rozwoju technologicznego i konsekwencji uzależnienia od technologii dla organizacji i rządów. Oczywiście zostaną poruszone również inne problemy: w niniejszym rozdziale przedstawiamy niektóre wydarzenia o największym znaczeniu; nie da się jednak uczynić tego w sposób wyczerpujący.

9.2. *Nadzór o charakterze innym niż technologiczny*

9.2.1. Podczas gdy większość uwagi skupia się na zaawansowanych technologiach nadzoru, nie należy zapominać, jak wiele podstawowych i bardzo ludzkich form nadzoru miało istotne znaczenie w całej historii, poczynając od starożytnego „podśluchiwania”, a także jak bardzo są one ważne we współczesnym społeczeństwie. Do form takich należą: prosta obserwacja, pilnowanie, słuchanie i śledzenie zarówno w ramach egzekwowania prawa, jak i przez osoby prywatne; wykorzystywanie szpiegów, tajnych współpracowników i informatorów przez policję i służby bezpieczeństwa; cała gama procedur z dziedziny medycyny, ubezpieczeń społecznych, finansów i rekrutacji opartych na bezpośrednich wywiadach i przechowywanie informacji w formie kartotek papierowych. Niektóre z najbardziej intensywnie działających systemów nadzoru w ustrojach autorytarnych opierały się właśnie na tych podstawowych składnikach, połączonych zazwyczaj z silnym poczuciem braku zaufania, obawą przed infiltracją, zatrzymaniem bądź wtargnięciem. Przykłady stanowią Niemcy i Japonia w czasach przed drugą wojną światową oraz kraje byłego bloku wschodniego, a zwłaszcza Niemiecka Republika Demokratyczna, która swego czasu zatrudniała w charakterze informatorów niemal jedną szóstą ludności.³⁴

9.2.2. Dwie inne rutynowe i zależne od człowieka formy nadzoru należą do tych, które mają największy wpływ na życie obywateli: sprawdzanie alkomatem osób podejrzanych o prowadzenie pojazdów w stanie nietrzeźwym i przeszukiwanie osób, które mogły brać udział w przestępstwach. Czynności te mogą obejmować zastosowanie technologii, ale zasadniczo opierają się na podejmowanej przez ludzi (funkcjonariuszy policji) decyzji, dotyczącej tego, kogo należy zatrzymać. Fakt, że decyzje takie opierają się na ocenie dokonywanej przez człowieka sprawia jednakże, że siły ścigania nie zajmują się jednakowo wszystkimi grupami społeczeństwa. Na przykład w Wielkiej

³⁴ Garton Ash, T. (1997) „*The File: A Personal History* [Archiwum: Historia osobista]”, New York: Vintage Books.

Brytanii prawdopodobieństwo zatrzymania i przeszukania czarnoskórego jest sześć razy wyższe niż białego człowieka.³⁵

9.2.3. Proste formy nadzoru mogą być bardziej skuteczne w zapewnianiu odpowiedniej ochrony i bezpieczeństwa niż metody oparte na technologiach. Na przykład w Wielkiej Brytanii kluczowym zagadnieniem jest brak jasnego stanowiska w sprawie pierwszoplanowego celu, w jakim ma być stworzony projektowany krajowy system potwierdzania tożsamości.³⁶ Nie jest nawet jasne, czy technologia ta przyczyni się do zwiększenia bezpieczeństwa w kraju. Lepsze wyniki można prawdopodobnie osiągnąć poprzez poprawę bezpieczeństwa na granicach i konwencjonalne gromadzenie danych wywiadowczych, o czym świadczy wykrycie w sierpniu 2006 roku planowanego zamachu terrorystycznego na samoloty przelatujące nad Atlantykiem, w którego przygotowaniu uczestniczyło ponad 20 Brytyjczyków.³⁷ Pomimo iż administracja USA dowodziła, że w trakcie operacji ujawniono potrzebę zgromadzenia znacznie bardziej szczegółowych danych na temat pasażerów,³⁸ planowany zamach został udaremniony dzięki wykorzystaniu informatorów, tajnych agentów i ostrzeżeń. Trudno wyobrazić sobie, w jaki sposób zaawansowane systemy potwierdzania tożsamości mogłyby przynieść lepsze efekty.

9.3. *Rozwój technologiczny*

9.3.1. Fakt, że nowe technologie pomogły zmienić charakter nadzoru, jest niepodważalny. Należy przytoczyć kilka ogólnych spostrzeżeń, dotyczących charakteru „technologii” nadzoru. Po pierwsze, w odniesieniu do tych systemów technologicznych nie istnieją cechy z definicji „złe” lub „dobre”. W ujęciu historycznym, wykorzystujące perforowane karty maszyny firmy IBM były równie istotnym elementem dla skutecznego funkcjonowania gigantycznego systemu nadzoru nad ludnością, który umożliwił nazistom wyszukanie, uwięzienie i eksterminację Żydów i innych „niepożądanych elementów”, jak wczesne komputery, dzięki którym złamano szyfry Enigmy, co przyspieszyło zwycięstwo aliantów nad nazistami. Wydajne państwowe bazy danych mogą być używane zarówno do świadczenia ukierunkowanych usług zdrowotnych, jak i do prześladowania przeciwników politycznych.

9.3.2. Jednakże sposób wykorzystywania technologii nadzoru nie jest prostym zagadnieniem. Wszystkie technologie opracowywane są przez pewne organizacje, z których każda ma określone cele. Pewne technologie mogą zostać przyswojone przez użytkowników – na przykład przesyłanie wiadomości tekstowych pomiędzy telefonami komórkowymi nigdy nie miało być głównym celem ich istnienia. Jednakże możliwości technologii uzależnione są od przypisanych jej przez konstruktorów założeń funkcjonalnych, jak to ma miejsce w przypadku wbudowanej funkcji śledzenia preferencji telewidzów w

³⁵ Home Office (2006) „Operational Policing – Impact: about the Programme [Policijne działania operacyjne – Wpływ: o programie]”, viiii. <http://police.homeoffice.gov.uk/operational-policing/impact/impact-about-the-programme/>

³⁶ House of Commons Select Committee on Science and Technology [Izba Gmin, Komisja ds. Nauki i Technologii] (2006) „Identity Card Technologies: Scientific Advice, Risk and Evidence [Technologie kart identyfikacyjnych: Poradnictwo naukowe, ryzyko i materiał dowodowy]”, http://www.parliament.uk/parliamentary_committees/science_and_technology_committee/sag.cfm

³⁷ Patrz: „Special report: terrorism threat to Britain [Raport specjalny: zagrożenie terroryzmem dla Wielkiej Brytanii]”, *The Guardian*, 2006, <http://www.guardian.co.uk/terrorism/0,,873826,00.html>

³⁸ „Government Seeks to Expand Data Collection on Airline Passengers [Rząd stara się poszerzyć zakres gromadzonych danych dotyczących pasażerów linii lotniczych]” 22 August (22 sierpnia) 2006, *New York Times*, <http://www.nytimes.com/2006/08/22/washington/22data.html?ex=1313899200&en=1985587a17e2fbaa&ei=5090&partner=rssuserland&emc=rss>

licznych systemach „telewizji na żądanie”, takich jak TiVo. Jak już to widzieliśmy, wiele technologii działa jako element globalnych sieci, a parametry tych sieci są kontrolowane przez korporacje, państwo, a często również przez wojsko, jak na przykład Globalny System Pozycjonowania (GPS).

- 9.3.3. Poniżej przedstawiamy kilka takich technologii oraz ich możliwości. Uwagę należy poświęcić nie tylko możliwościom i praktycznemu wykorzystaniu danej technologii, ale także procesowi jej powstawania, kontroli nad jej funkcjonowaniem w charakterze części sieci i sposobowi, w jaki łączy się ona z innymi technologiami.

9.4. *Telekomunikacja*

- 9.4.1. Nadzór w telekomunikacji odnosi się do zakresu, w jakim organizacje i osoby prawne są w stanie monitorować, klasyfikować i przechowywać informacje dotyczące przebiegu i zawartości wymiany wiadomości przesyłanych przez sieć telekomunikacyjną, zarówno pomiędzy urządzeniami technicznymi, jak i pomiędzy urządzeniami technicznymi a ludźmi. „Telekomunikacja” obejmuje infrastrukturalne, technologiczne procesy komunikacji, systemy i urządzenia, za pośrednictwem których uzyskiwane są połączenia, jak również dokonywana jest wymiana „danych”, „wiadomości” lub „informacji”. Obecna definicja telekomunikacji obejmuje nie tylko analogowe, ale też cyfrowe formaty sygnału, a system telekomunikacyjny to nie tylko stacjonarna telefonia kablowa z możliwością komunikacji głosowej i przesyłania telefaksów czy telefonia komórkowa, ale również bardzo szeroka gama funkcji komunikacyjnych, jakie spełniają cyfrowe i informatyczne systemy o ogromnym zasięgu, takie jak Internet.

- 9.4.2. W ujęciu historycznym, infrastruktura telekomunikacji w Wielkiej Brytanii była zdominowana przez stacjonarną telefonię kablową, której operatorem była General Post Office [Pocztą]. Jedynym najbardziej prawdopodobnym źródłem nadzoru był podsłuch telefoniczny, najczęściej związany z egzekwowaniem prawa przez państwo. Trzy główne wydarzenia doprowadziły do gwałtownej przemiany tego systemu: ekspansja i konwergencja technologii telekomunikacyjnych, rozwój technik przechowywania informacji i zdolności przetwarzania oraz zróżnicowanie rynków telekomunikacyjnych.

- 9.4.3. W ciągu ostatnich dwóch dekad rozwój technologiczny i zmiany doprowadziły do powstania bardziej zróżnicowanych technologii, które zastosowano w telekomunikacji. Na przykład urządzenia pracujące na częstotliwościach fal radiowych umożliwiają obecnie funkcjonowanie na skalę masową telefonii komórkowej lub mobilnej;³⁹ kable z włóknami optycznymi umożliwiają działanie stacjonarnych, cyfrowych połączeń internetowych o dużej szybkości. Dzięki połączeniu tych dwóch technologii działają bezprzewodowe systemy informatyczne. Telefonia komórkowa umożliwia nie tylko wykonywanie połączeń głosowych, ale również przesyłanie wiadomości tekstowych i obrazów, jak również korzystanie z usług opartych na lokalizacji.⁴⁰ Technologie internetowe umożliwiają zarówno stosowanie asynchronicznych środków komunikacji, takich jak poczta elektroniczna,

³⁹ Radio umożliwia również funkcjonowanie technologii RFID (identyfikację częstotliwości radiowych), służącej do śledzenia towarów, usług i – potencjalnie – ludzi.

⁴⁰ Usługi oparte na lokalizacji w telefonii komórkowej obejmują globalne, satelitarne systemy przekazywania informacji i pozycjonowania.

elektroniczne tablice ogłoszeń i grupy dyskusyjne (newsgroups), jak i środków synchronicznych, takich jak zorganizowane spotkania w sieci (chatroom), wymiana wiadomości na bieżąco oraz przesyłanie wiadomości za pośrednictwem kamer internetowych lub kamer wideo.⁴¹ Ponadto, zachodzące obecnie w technologiach komunikacji zmiany obejmują zarówno równoległy rozwój technologii, jak i zdolność tych technologii do wzajemnej współpracy. Połączenia internetowe mogą obecnie być dokonywane za pośrednictwem całego szeregu urządzeń, począwszy od urządzeń mieszczących się w ręku i telefonów komórkowych. Wraz z pojawieniem się opcji VoIP (połączenia głosowe za pośrednictwem protokołu internetowego) połączenia głosowe mogą być realizowane za pośrednictwem zwykłego komputera osobistego.

9.4.4. Wraz z rozwojem każdej z tych technologii pojawiały się mechanizmy służące do wykorzystania ich do nadzoru. Do funkcjonowania każdej z tych technologii niezbędna jest wymiana sygnałów lub danych pomiędzy urządzeniami. Każda taka wymiana danych z natury rzeczy prowadzi do powstania mechanizmów służących do przechwytywania, monitorowania i przechowywania informacji dotyczących takiej wymiany.

9.4.5. Na przykład w telefonii komórkowej położenie urządzenia mobilnego (telefonu) może zostać określone poprzez triangulację emitowanego przez urządzenie sygnału z jego odbiorem przez kilka różnych stacji przekąźnikowych, ponieważ sygnały są przekazywane z jednej stacji do drugiej. Informacje takie można przechowywać, aby móc później pozyskiwać dane. Ponieważ wszystkie technologie telekomunikacyjne stają się w coraz większym stopniu zdolne do współpracy, zwiększa się ich zasięg i rośnie zagęszczenie, zwiększają się również wyraźnie możliwości w zakresie zbierania informacji, prowadzenia nadzoru, jak również przechowywania i pozyskiwania informacji uzyskanych dzięki tym technologiom. *Rutynowe* i zautomatyzowane gromadzenie danych na taką skalę ma miejsce zarówno w przypadku telefonów stacjonarnych, jak i połączeń internetowych (dane dotyczące telekomunikacji internetowej przechowywane na serwerach dostawców usług internetowych). Ponadto, w lutym 2006 roku dyrektywa UE w sprawie przetwarzania danych i inicjatywy ustawodawcze Home Office zawierały propozycje, aby wymagać przechowywania danych przez okres do dwóch lat nie tylko od firm telekomunikacyjnych, ale również od firm oferujących zarówno usługi telefonii stacjonarnej, jak i łącza internetowe. Dane te byłyby dostępne dla organów ścigania celem przeprowadzenia kontroli.

9.4.6. Ponadnarodowy państwowy nadzór telekomunikacyjny i wywiad elektroniczny (SIGINT) pozostaje owiany tajemnicą, a na temat jego możliwości technicznych krążą różne pogłoski, snuje się uczone domysły i ekstrapolacje. Państwo filtruje również rutynowo wielką liczbę połączeń telefonicznych, poczty elektronicznej i faksów z uwagi na „dobro państwa” (chodzi tu zarówno o bezpieczeństwo, jak i o interes gospodarczy). System zwany „ECHELON” – globalna sieć nadzoru amerykańskiej Agencji Bezpieczeństwa Narodowego (National Security Agency – NSA) – posiada olbrzymią siedzibę w Menwith Hill w Północnym Yorkshire. System ten rutynowo filtruje wszystkie połączenia telekomunikacyjne przechodzące przez Wielką Brytanię pod kątem kluczowych słów i wyrażeń i w coraz szerszym zakresie stosuje skomplikowane algorytmy do rozpoznawania słów, a nawet ich

⁴¹ Takie funkcje internetu, jak strony internetowe i blogi (dzienniki sieciowe) zostały w niniejszym raporcie pominięte, ponieważ są one szeroko „publikowane” i stąd też są w sposób oczywisty ogólnie dostępne.

znaczenia⁴². Komunikacja za pośrednictwem tzw. międzynarodowej sieci kablowej (International Licensed Cable – ILC) są najprawdopodobniej jedną z najłatwiejszych do przechwycenia form komunikacji, ponieważ z przyczyn historycznych wszystkie linie przechodzą przez znajdujące się w większych miastach punkty węzłowe. Dlatego też jednym z głównych centrów przechwytywania komunikacji odbywającej się za pośrednictwem ILC jest Londyn. Dokonuje tego brytyjska Kwatera Główna ds. Komunikacji (GCHQ - General Communications Headquarters), przy użyciu olbrzymiego komputera, znanego pod nazwą Dictionary (Słownik).

9.5. Nadzór wideo

9.5.1. Nadzór fotograficzny istnieje dłużej, niż sądzi większość ludzi. Niemal od razu po wynalezieniu aparatu fotograficznego zaczęto go używać do rejestracji twarzy i innych cech fizycznych przestępców.⁴³ Nawet wykorzystujący kamery telewizyjne i system nadzoru wideo zwany telewizją przemysłową (CCTV) funkcjonuje tymczasowo w przestrzeniach publicznych Wielkiej Brytanii już od czasu koronacji królowej Elżbiety II w 1953 roku, a na stałe w niektórych częściach Londynu – od końca lat 60-tych XX wieku⁴⁴.

9.5.2. Po niedawnym wzroście liczby zainstalowanych systemów CCTV, jaki miał miejsce począwszy od wczesnych lat 90-tych w związku z próbami zapobieżenia upadkowi dzielnic handlowych w centrach miast oraz obawą przed terroryzmem i przestępczością, liczba kamer CCTV w Wielkiej Brytanii mogła osiągnąć poziom około 4,2 miliona sztuk, czyli jedna na czternaście osób⁴⁵. Pojedynczy człowiek może zostać zarejestrowany w ciągu dnia nawet przez 300 takich kamer.⁴⁶

9.5.3. W latach 90-tych Home Office wydało na instalację systemów telewizji przemysłowej⁴⁷ 78% budżetu przeznaczonego na zapobieganie przestępczości, co w skali dziesięciolecia daje kwotę około 500 milionów funtów zainwestowanych w infrastrukturę CCTV.⁴⁸ Jednakże sporządzone przez Home Office studium zawiera wniosek, że „oceniane systemy CCTV miały ogólnie niewielki wpływ na poziom przestępczości”.⁴⁹

9.5.4. Wprowadzenie formatów cyfrowych umożliwia w coraz większym stopniu zautomatyzowane wykorzystanie systemów CCTV. Jak dotychczas

⁴² Campbell, D. (1999) „*Development of Surveillance Technology and Risk of Abuse of Economic Information (An appraisal of technologies of political control)* [Rozwój technologii nadzoru i ryzyko nadużycia informacji gospodarczych (ocena technologii kontroli politycznej)]” Tom 2/5: *Interception Capabilities 2000*, Luksemburg: Parlament Europejski, Dyrekcja Generalna ds. Badań, Dyrekcja A, Program STOA; Wood, D (2001) „*The Hidden Geography of Transnational Surveillance*, Unpublished PhD Thesis [Ukryta geografia nadzoru ponadnarodowego – niepublikowana praca doktorska]”, University of Newcastle, Wielka Brytania.

⁴³ Sekula, A. (1986) „*The Body and the Archive [Ciało i archiwum]*” *October* 39: s. 3-64; Finn, J. (2004) „*Photographing fingerprints: data collection and state surveillance [Fotografowanie odcisków palców: zbieranie danych i nadzór ze strony państwa]*”, *Surveillance & Society* 3(1): s. 21-44. [http://www.surveillance-and-society.org/Articles3\(1\)/fingerprints.pdf](http://www.surveillance-and-society.org/Articles3(1)/fingerprints.pdf)

⁴⁴ Williams, C. A. (2003) „*Police surveillance and the emergence of CCTV in the 1960s [Nadzór policyjny i powstanie CCTV w latach 60-tych]*”, *Crime Prevention and Community Safety* 5(3): s. 27-38.

⁴⁵ McCahill, M. and Norris, C. (2003), „*Estimating the extent, sophistication and legality of CCTV in London [Ocena zakresu, złożoności i legalności CCTV w Londynie]*”, w: M. Gill (wyd.) *CCTV*, Perpetuity Press.

⁴⁶ Norris, C i Armstrong, G. (1999), „*The Maximum Surveillance Society: The Rise of Closed Circuit Television [Społeczeństwo maksymalnego nadzoru: Powstanie telewizji przemysłowej]*”, Oxford: Berg.: s. 42

⁴⁷ *tamże*: s. 54

⁴⁸ Norris, C. (2006) „*Closed Circuit Television: a review of its development and its implications for privacy [Telewizja przemysłowa: przegląd jej rozwoju i jej skutki dla prywatności]*”, dokument przygotowany na ciekawostkę spotkanie Komitetu Doradczego Departamentu ds. Bezpieczeństwa Wewnętrznego, Ochrony i Rzetelności Danych (Department of Homeland Security Data Privacy and Integrity Advisory Committee), 7 czerwca, San Francisco CA.

⁴⁹ Gill, M. i Spriggs, A. (2005). „*Assessing the impact of CCTV [Ocena wpływu CCTV]*”. London, Home Office Research, Development and Statistics Directorate [Dyrekcja ds. Badań, Rozwoju i Statystyki, Ministerstwo Spraw Wewnętrznych, Londyn], 43, s. 60-61.

dotyczy to w większości dróg. Tablice rejestracyjne służą do identyfikacji zarejestrowanego właściciela samochodu. Liczba przypadków ścigania za przekroczenie ograniczeń prędkości wynosiła w roku 1996 nieco ponad 300000. W roku 2004 liczba ta wyniosła już ponad 2 miliony, a przychody uzyskane z kar kształtują się na poziomie 113 milionów funtów rocznie.⁵⁰ Takie nasilenie nadzoru ze strony państwa spotyka się niezmiennie z negatywnymi ocenami ze strony mediów⁵¹ pomimo faktu, że kamery do pomiaru prędkości, w odróżnieniu od ulicznych systemów CCTV mają istotny wpływ na zmniejszenie liczby zabitych i rannych w wypadkach drogowych.⁵²

- 9.5.5. Proces intensyfikacji nadzoru ruchu drogowego postępuje bardzo szybko. W marcu 2005 Stowarzyszenie Komendantów Policji (Association of Chief Police Officers) wystąpiło z wnioskiem o stworzenie systemu Automatycznego Rozpoznawania Tablic Rejestracyjnych (ANPR – Automatic Number Plate Recognition) „wykorzystującego kamery należące do policji, władz lokalnych, Agencji ds. Autostrad (Highways Agency), innych partnerów oraz sektora komercyjnego”⁵³. W ramach tego systemu ma dojść do integracji zainstalowanych w centrach miast i na głównych ulicach⁵⁴ kamer z Krajowym Centrum Danych ANPR o zdolności operacyjnej pozwalającej na przetworzenie 35 milionów odczytów ANPR dziennie. Zdolność ta ma wzrosnąć do 50 milionów w 2005 roku, przy czym okres przechowywania danych ma wynosić 2 lata.

9.6. Baza danych

- 9.6.1. Być może to właśnie zdolność przechowywania spowodowała największą zmianę powstałą w wyniku rewolucji technicznej: wszechobecność komputerowej bazy danych. Obecnie różne dane mogą być gromadzone, zestawiane i łączone znacznie szybciej i dokładniej, niż za pomocą papierowych kartotek, które niegdyś stanowiły charakterystyczną cechę nowoczesnej biurokracji.

- 9.6.2. Gromadzenie, wykorzystywanie i udostępnianie dużych zbiorów danych osobowych dotyczących obywateli ma obecnie kluczowe znaczenie dla funkcjonowania przedsiębiorstw prywatnych i służb publicznych. Różne zestawy danych mogą być porównywane z innymi w celu identyfikacji osób i podejrzanych wzorów zachowań. Dane mogą być również „poddawane eksploracji”, czyli dogłębnej analizie przeprowadzanej za pomocą wyszukanych technologii w celu ujawnienia modeli, które wymagają dalszego dochodzenia.

- 9.6.3. Nadzór, jaki wiąże się ze służbami publicznymi może być rozumiany jako „nadzór danych”, „systematyczne wykorzystanie systemów danych osobowych w dochodzeniu lub monitorowaniu działań lub komunikacji jednej

⁵⁰ Wilkins, G. i Addicott, C. (1998) „*Motoring Offences England and Wales 1996* [Przestępstwa drogowe w Anglii i Walii 1996]”, Home Office Statistical Bulletin, London: Home Office; Ransford, F., Perry, D. Murray, L. (2005) „*Motoring Offences and Breath Test Statistics: England and Wales 2003* [Przestępstwa drogowe i statystyki badań wydychanego powietrza: Anglia i Walia 2003]”, Home Office Statistical Bulletin, London: Home Office.

⁵¹ McCahill i Norris, 2003 *op cit.* n.

⁵² PA Consulting (2004) „*Denying Criminals the Use of the Road* [Zakazać przestępcom korzystania z dróg]”, http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/ANPR_10,000_Arrests.pdf?view=Binary

⁵³ *tamże*, s. 6.

⁵⁴ *tamże*, s. 18

lub większej liczby osób”.⁵⁵ Wyrażenie to, w którego skład wchodzi słowo „nadzór”, zwraca uwagę na większe znaczenie baz danych, niż służących do pilnowania ludzi środków audiowizualnych, jakie stosowane są w państwach i przedsiębiorstwach. Bazy danych w połączeniu z innymi systemami nadzoru umożliwiają także nadzór algorytmiczny, wykorzystywanie programów komputerowych służących do pracy z zarejestrowanymi obrazami lub danymi i porównywanie ich z danymi znajdującymi się w bazie danych. Miało to zasadnicze znaczenie w rozwoju biometrii (patrz poniżej).

9.6.4. W sektorze prywatnym malejące koszty baz danych i zwiększająca się zdolność uzyskiwania z danych informacji i wartości, dających podstawę do prowadzenia dochodzenia na drodze sądowej, miały wpływ na gospodarkę danymi osobowymi, z której wiele korporacji stara się uzyskać jak najwięcej danych o konsumentach.⁵⁶ Dane dotyczące konsumentów można podzielić na cztery kategorie⁵⁷: *Dane geograficzne*, które opisują cechy miejsca, wskazywane za pomocą telefonicznych numerów kierunkowych, kodów pocztowych, adresów internetowych URL i nazw domen. Dane te są prawie zawsze związane z *danymi demograficznymi*, dotyczącymi danych osób i znane są pod nazwą „dane geodemograficzne”. *Dane psychograficzne* dotyczą bardziej społecznych aspektów życia konsumentów, a mianowicie klasy, wartości, stylu życia, etapu życia i osobowości. W końcu istnieje kategoria danych dotyczących *zachowań konsumentów*.

9.6.5. Istnieje wiele sposobów tworzenia i gromadzenia danych. Każda transakcja dostarcza „śladu danych” (data trail), umożliwiającego powiązanie z daną osobą lub kategorią osoby.⁵⁸ Na takie transakcje składają się te, które są dokonywane za pomocą kart kredytowych, kart bankomatowych, telefonów komórkowych, Internetu, czyli związane z robieniem zakupów, korzystaniem z Internetu czy prowadzeniem rozmowy telefonicznej. Dodatkowe dane są generowane za pomocą kart programów lojalnościowych, badań konsumentów, zogniskowanych wywiadów grupowych, konkursów promocyjnych, próśb o przekazanie informacji na temat produktu, kontaktów z telefonicznym centrum obsługi klienta, plików cookies, internetowych forów konsumenckich i transakcji kredytowych. Te dane *wewnętrzne*, będące na ogół danymi zastrzeżonymi, nakładają się często z danymi *zewnętrznymi*, pochodzącymi z agencji państwowych (np. krajowego urzędu statystycznego), organizacji pozarządowych lub firm specjalizujących się w gromadzeniu danych. Ten szybko rozwijający się sektor gospodarki gromadzi dane łącząc dane publicznie dostępne (na przykład pochodzące ze spisu ludności lub książki telefonicznej) z danymi pochodzącymi z konkursów promocyjnych, informacji gwarancyjnych (uzupełnionych szeroko zakrojonymi badaniami), badań prowadzonych w systemie *door to door*, przez telefon i osobiście w centrach handlowych, jak również z danymi pochodzącymi z umów na dostarczanie usług telekomunikacyjnych i informacyjnych oraz śladów związanych z odwiedzaniem stron internetowych. Te łatwo jest powiązać z kodami pocztowymi, przy czym ulice są przyporządkowane do pewnych kategorii,

⁵⁵ Clarke, R. (1991 [1987]) „Information technology and dataveillance [Technologia informacji i nadzór danych]”, <http://www.anu.edu.au/people/Roger.Clarke/DV/CACM88.html>

⁵⁶ Zob. Dyson, E., Gilder, G., Keyworth, G. and Toffler, A. (1996) „Cyberspace and the American dream [Cyberprzestrzeń i amerykański sen]” *The Information Society* 12: 295-308; 6, P. (2005) „The personal information economy: trends and prospects for consumers [Gospodarka informacji osobowych, tendencje i perspektywy dla konsumentów] w Lace, S. (wyd.) (2005) *op cit.* nr 6.

⁵⁷ Kategorie te pochodzą z: Michman, R.D. (1991) *Lifestyle Market Segmentation [Segmentacja rynku ze względu na styl życia]*. New York: Praeger; zob. również: Elmer, G. (2004) *Profiling Machine [Formatyzerki]*. Cambridge, MA: MIT Press.

⁵⁸ Na przykład transakcje gotówkowe, mimo że na ogół nie jest możliwe ich bezpośrednie powiązanie z konsumentem, często są analizowane na podstawie wcześniejszych transakcji i rodzajów konsumentów, którzy dokonali takich zakupów.

nazywanych profilami, jak na przykład „prudent pensioners” (ostrożni emeryci), „fledgling nurseries” (żłobki) i „rustbelt resilience (odbudowujące się upadłe obszary przemysłowe)”.⁵⁹ Profile dostarczają firmom środki umożliwiające kierowanie działań marketingowych do węższej grupy konsumentów, na przykład, bank posiadający umowę z biurem podróży może wprowadzać na rynek inną ofertę wakacji rodzinnych dla osób przypisanych do profilu „rodziny”, a inną dla profilu „emeryci”.⁶⁰ Podmioty trzecie także mogą dostarczać wykazy konsumentów, których pasjonuje ogrodnictwo (prawdopodobnie na podstawie prenumeraty prasy specjalistycznej) lub częste podróże (prawdopodobnie na podstawie przeprowadzonych badań). Powiązania ustanowione między zestawami danych są wynikiem technik „eksploracji danych”, których celem jest uzyskanie „grupy” danych wskazujących na formy i zależności w konkretnym zestawie danych.

9.6.6. Proste techniki łączenia danych oraz wykorzystywanie profili geodemograficznych zostało obecnie poszerzone o bardziej wyszukane heurystyczne procesy eksploracji danych, często określane jako „odkrywanie wiedzy w bazach danych” (Knowledge Discovery in Databases (KDD)). Pomaga to poza tym w odkrywaniu uprzednio nieznanych i *nieoczywistych* zależności w zestawach informacji.⁶¹ „Produkt” tych systemów jest być może najbardziej widoczny, jako że jest podstawą systemów personalizacji internetowej, stosowanej przez Amazon.com, wykorzystującej różne źródła danych w celu określenia prawdopodobnych dzisiejszych upodobań klientów.⁶² Techniki te pozwalają zarówno na opis wzorców zachowań, jak i prognoz dotyczących zachowania w rozsądnym zakresie dokładności. Przyjmując, że dany klient będzie naśladował zachowania innych w zależności lub niezależnie od tego, czy są one oczywiste czy nie. Takie modele zachowania konsumenta służą do pokazania skłonności konsumentów do nabywania pewnych produktów, odpowiedzi na niektóre kampanie reklamowe, zmniejszenia siły nabywczej lub zjawiska ryzyka kredytowego, itd.

9.6.7. Rozwój i wykorzystywanie bazy danych stanowi kluczowy element zmian w sektorze usług publicznych. Miały miejsce na przykład duże inwestycje promujące wykorzystywanie danych osobowych w dziedzinie opieki zdrowotnej. Program IT brytyjskiej państwowej służby zdrowia (NHS) noszący nazwę *Connecting for Health* (łączenie dla zdrowia) jest największym w Europie, a podjęte zobowiązania sięgają daleko w przyszłość.⁶³ Podczas ubiegłej dekady poczyniono wiele wysiłków mających na celu koordynację i rozwój elektronicznej karty pacjenta (EPR), zmierzając w ostatnim czasie w

⁵⁹ Poprzednia kategoria pochodzi z systemu klasyfikacji ACORN firmy znanej jako CACI, a dwie kolejne kategorie pochodzą z klasyfikacji MOSAIC Experian. Więcej informacji o tych produktach można uzyskać pod adresem: <http://www.caci.co.uk/acorn/> i <http://www.business-strategies.co.uk/Content.asp?ArticleID=629> Patrz również: Burrows, R. and Gane, N. (w przygotowaniu) „Geodemographics, software and class [Geodemografia, oprogramowanie i klasa]” *Sociology*.

⁶⁰ Co więcej, istnieją ograniczenia związane z prywatnością odnoszące się do tych informacji i wymiany ich między firmami, w związku z tym że pewne klauzule pozwalają na taką praktykę, w szczególności jeśli materiały marketingowe pochodzą bezpośrednio od właściciela danych, którym w tym przypadku jest bank.

⁶¹ W celu uzyskania dalszych informacji na temat rozróżnienia między KDD i eksploracji danych, zob. Tavani, H.T. (1999) „KDD, data mining, and the challenge for normative privacy [KDD, eksploracja danych i wyzwanie dla normatywnej prywatności]” *Ethics and Information Technology* 1: 265-273. Wiele źródeł traktuje eksplorację danych jako ogólny proces pracy z danymi dla potrzeb tu opisanych. zob. Rygielski, C., Wang, J-C i Yen, D.C. (2002) „Data mining techniques for Customer Relationship Management [Techniki eksploracji danych dla zarządzania relacjami z klientami]” *Technology in Society* 24: 483-502, Danna i Gandy (2002) *op cit.* nr 6. W celu wyjaśnienia, termin KDD jest tu stosowany w celu zdefiniowania ogólnego technicznego procesu, który wskazuje na szczególne podobieństwa (oczywiste bądź nie) w kontekście zestawów danych i eksploracji danych, jako praktyk gromadzenia danych krytycznych dla potrzeb przyszłych analiz danych.

⁶² Fink, J. i Kosba, A. (2000) „A review and analysis of commercial user modeling servers for personalization on the World Wide Web [Badanie i analiza komercyjnych serwerów modelowania użytkowników na www]” *User Modeling and User-Adapted Interaction* 10: 209-249.

⁶³ The Wanless Report (2002) *Securing Our Future Health: Taking a Long-Term View: Final Report [Chronicząc nasze zdrowie w kontekście perspektywy długoterminowej]*, London: H.M.Treasury.

kierunku ogólnokrajowej cyfrowej bazy danych wszystkich indywidualnych kart zdrowia. Podstawowy zestaw danych NHS na temat każdego pacjenta⁶⁴ znajduje się w centralnym rejestrze służby zdrowia (Care Records Service) funkcjonującym przy NHS i zawiera ograniczoną ilość podstawowych informacji, które mogą zostać powiązane z dużą ilością lokalnych informacji dotyczących opieki zdrowotnej. Ponadto program obejmuje krajowe bazy danych zawierające karty pacjenta dostarczane przez lokalne jednostki NHS, w tym dane na temat chorób podlegających obowiązkowi zgłaszania i informacje przechowywane na potrzeby audytu klinicznego. Diagnostyka laboratoryjna i inne karty badań mogą być wypełniane elektronicznie. Plany, częściowo już wprowadzone, obejmują także rezerwacje wizyt, recepty, elektroniczny transfer kart pacjenta między lekarzami pierwszego kontaktu oraz inne funkcje. Elektroniczne karty pacjenta są przekazywane w sposób bezpieczny, ponieważ zakodowane są za pomocą systemu kryptografii klucza publicznego i podlegają zasadom, które umożliwiają pracownikom każdej jednostki NHS na korzystanie tylko z tych danych, które są im potrzebne. Zostało opracowanych kilka lokalnych programów pilotażowych, w ramach których pacjenci mogli zarządzać własnymi danymi za pomocą kart chipowych.

9.6.8. Bazy danych mają także duże znaczenie w kontekście egzekwowania prawa. Angielska i walijska policja rocznie aresztuje około dwóch milionów osób. Ustawa o prawie karnym (Criminal Justice Act) z 2003 r. nadała policji prawo do pobierania od osób aresztowanych odcisków palców i próbek DNA, które pozostają w policyjnych bazach danych i są dostępne w krajowym komputerowym systemie policyjnym niezależnie od tego, czy wina została dowiedziona, czy też nastąpiło uniewinnienie. Bazy danych odcisków palców obecnie zawierają blisko 6 milionów odcisków palców, a ich automatyczne dopasowywanie jest prawie natychmiastowe.⁶⁵ Krajowa baza danych DNA została założona w 1995 r. i rozwinęła się na tyle, że „praktycznie cały aktywny świat przestępczy do 2005 r. powinien znaleźć się w bazie danych”.⁶⁶ W grudniu 2005 r. w bazie danych znajdowało się 3,45 miliona profili osób, co stanowiło mniej więcej 5,2% całej ludności. W bazie danych znajduje się blisko 40% profili mężczyzn należących do rasy negroidalnej, 9% mężczyzn należących do rasy białej a 13% do rasy żółtej.⁶⁷ Ustawa o narkotykach (Drugs Act) z 2005 r., która zaczęła obowiązywać w marcu 2006 r., dała policji prawo do poddawania badaniom na obecność narkotyków wszystkich osób, które zostały aresztowane za przestępstwa związane z narkotykami, w tym kradzież, rozbój, kradzież z włamaniem i żebranie, również niezależnie od tego, czy wina została udowodniona czy też nie.

9.6.9. Sercem policyjnej infrastruktury IT jest państwowy komputerowy system policyjny (Police National Computer PNC). Państwowy komputerowy system policyjny przechowuje wiele baz danych i umożliwia korzystanie z zewnętrznych baz danych, takich jak rejestry kierowców prowadzone przez wydział komunikacji DVLC, a obecnie jest połączony z ponad 30 000 terminali w całym kraju. W ciągu ostatniej dekady państwowy komputerowy system policyjny rozwinął się; z elektronicznego segregatora stał się w pełni inteligentnym narzędziem umożliwiającym wyszukiwanie w każdej z

⁶⁴ NHS Connecting for Health (2006) 'spine', <http://www.connectingforhealth.nhs.uk/delivery/programmes/spine>.

⁶⁵ PITO (Police Information Technology Organisation – Organizacja ds. policyjnych technologii informacyjnych) (2005) *Annual Report 2004 – 2005*, HC 261, London Stationery Office.

⁶⁶ FSPU (Forensic Science and Pathology Unit – jednostka medycyny sądowej i diagnostyki laboratoryjnej) (2005) *DNA Expansion Programme 2000-2005: Reporting Achievement [Program rozwoju DNA 2000-2005: wyniki]* London Home Office:3, Postnote 200.

⁶⁷ Randerson, J., „DNA of 37% of black men held by police [DNA 37% mężczyzn należących do rasy negroidalnej zatrzymanych przez policję]”, *The Guardian*, 5 stycznia 2006 r., <http://www.guardian.co.uk/frontpage/story/0,1678168,00.html>.

dziedzin.⁶⁸ Obecnie został on powiększony o system ANPR, Automatyczny System Identyfikacji Odcisków Palców (NAFIS) oraz Rejestr sprawców przestępstw z użyciem przemocy i na tle seksualnym (ViSOR), dostarczając tym samym policji i kuratorom wspólną krajową bazę danych, zawierającą obszerne zestawy informacji na temat przestępców, w tym dane personalne, dane opisowe, dane dotyczące zachowania, szczegóły oceny zagrożenia, raporty wywiadowcze, dziennik zdarzeń i zdjęcia⁶⁹. Najnowszą inicjatywą jest projekt, mający na celu rozwinięcie krajowej bazy danych zdjęć twarzy (FIND), posiadającej odniesienia do państwowego komputerowego systemu policyjnego, tak aby można było z niej w pełni korzystać do 2009 r.⁷⁰ Bazy danych są także wykorzystywane do kontroli rejestrów skazanych, które są obecnie niezbędne w przypadku osób szukających zatrudnienia w sektorze związanym z opieką nad osobami młodymi lub bezbronnymi. Od 2002 r. miało miejsce 8,2 miliona przypadków udostępnienia danych, z czego 400 000 zawierało wyroki skazujące lub informacje wywiadu policyjnego.⁷¹ Zostaną one połączone w systemie wymiany informacji na temat przestępstw (Criminal Justice Exchange, CJX), umożliwiającym wymianę informacji między jednostkami wymiaru sprawiedliwości⁷², nie tylko na komisariatach policji, ale także, wraz z rozwojem systemu Airwave, nowego systemu cyfrowej komunikacji brytyjskiej policji, między ulicznymi patrolami policyjnymi wyposażonymi w przenośne komputery.⁷³ Ostatecznie, projekt międzyregionalnej wymiany informacji (CRISP) stworzy jedną krajową policyjną bazę danych, która połączy wszystkie bazy danych w krajowym komputerowym systemie policyjnym z lokalnymi bazami danych.⁷⁴

9.6.10. Wraz z rozwojem krajowej strategii ANPR, baza danych została ustanowiona po to, aby stać się jeszcze bardziej centralnym elementem rutynowego pilnowania porządku publicznego. Na przykład w ramach strategii ANPR opracowany został plan podłączenia do systemu kamer zainstalowanych na parkingach warsztatów samochodowych, co znacznie zwiększy zasięg systemu, ponieważ wszystkie pojazdy w jakimś momencie muszą zatankować benzynę. Z kolei stacje benzynowe „skorzystają z tych informacji, dzięki czemu będą wiedziały od których pojazdów należy pobierać opłatę przed ich obsłużeniem”⁷⁵.

9.6.11. W przypadku obaw związanych z praktykami nadzoru granicznego miała miejsce znacząca zmiana roli straży granicznej zorientowana na dane. Szybki wzrost liczby „inteligentnych granic” (smart borders) i „elektronicznych granic” ma na celu zmienianie pozycji straży granicznych, jako "ostatniej, a nie

⁶⁸ *ibid.*

⁶⁹ PITO (2004) „Memorandum by the Police Information Technology Organisation to the Bichard Inquiry [Memorandum organizacji ds. policyjnych technologii informacyjnych dla Bichard Inquiry]”, http://www.bichardinquiry.org.uk.edgesuite.net/10663/full_evidence/0018/00180001.pdf.

⁷⁰ PITO (2006) *Facial Images National Database [krajowa baza danych obrazów twarzy] (FIND)*, <http://www.pito.org.uk/products/FIND.php>

⁷¹ „Criminal records mix-up uncovered [Ujawnienie zamieszania z rejestrami kryminalnymi]”, *BBC News*, 21 May 2006, <http://news.bbc.co.uk/1/hi/uk/5001624.stm>

⁷² CJIT (Criminal Justice Information Technology- technologia informacyjna wymiaru sprawiedliwości) (2005) *CJS Exchange*, <http://www.cjit.gov.uk/glossary/#c>

⁷³ ACPO (Association of Chief Police Officers - stowarzyszenie komendantów policji) (2002) *Infinet: A National Strategy for Mobile Information [Infinet, krajowa strategia łączności mobilnej]*, London: ACPO.

⁷⁴ Home Office (Ministerstwo Spraw Wewnętrznych Wielkiej Brytanii) (2006) *op cit.* nr 34.

⁷⁵ ACPO (Association of Chief Police Officers- stowarzyszenie komendantów policji) (2005) *ANPR Strategy for the Police Service 2005-8: Denying Criminals the Use of the Road [Strategia ANPR dla policji na lata 2005/08: odmawianie przestępcom możliwości korzystania z dróg]*, London: ACPO. http://www.acpo.police.uk/asp/policies/Data/anpr_strat_2005-08_march05_12x04x05.doc

pierwszej linii obrony".⁷⁶ Codzienne czynności związane z prowadzeniem nadzoru na granicy są poprzedzane działaniami systemu nadzoru danych, który ocenia stopień ryzyka zanim następuje fizyczna kontrola graniczna.

- 9.6.12. Nie chodzi tu wyłącznie o przemieszczanie się ludzi, ale również o przepływ pieniędzy i towarów.⁷⁷ Do obowiązków specjalnej grupy zadaniowej ONZ, znanej pod nazwą „Financial Action Task Force” (FATF), zajmującej się przechwytywaniem środków finansowych organizacji terrorystycznych, należy na przykład zatrzymywanie pieniędzy zanim te dotrą do granicy. Zgodnie z wynikami przeprowadzonych analiz, walka z przekazywaniem środków finansowych należących do organizacji terrorystycznych spowodowała nasilenie się nadzoru prowadzonego przez firmy zajmujące się międzynarodowymi przekazami pieniężnymi, takie jak Western Union, tym samym nadzoru nad pieniędzmi przekazywanymi przez imigrantów do krajów, z których pochodzą. Ważnym zagadnieniem jest sposób, w jaki dane są wykorzystywane do przeprowadzenia wstępnej oceny ryzyka dotyczącego szczególnych przypadków przekraczania granicy, a także tego, kogo w największym stopniu dotyczą takie oceny.

9.7. *Biometria*

- 9.7.1. Wszystkie nowe systemy identyfikacji tożsamości wykorzystują informacje biometryczne, takie jak na przykład odciski palców, skany tęczówki, topografia twarzy i skany dłoni – wszystkie one są wykorzystywane w różnych paszportach i systemach opierających się na dowodach tożsamości. Urok danych biometrycznych polega na tym, że wydają się być „kotwicą” dla tożsamości ciała ludzkiego, do której można przymocować dane i informacje. Identyfikator biometryczny – skan tęczówki, cyfrowe odciski palców, skany twarzy, głos i skan dłoni – staje się bramą dostępu do posiadanych danych. Jest to zbieżność eksploracji danych i integracji informacji z identyfikatorami biometrycznymi. Celem tych zabiegów jest zwiększenie dokładności i zmniejszenie liczby oszustw. Numery PIN i hasła można zapomnieć lub zgubić, a ciało człowieka zapewnia stały bezpośredni związek między danymi w rejestrach a osobą.

- 9.7.2. W sytuacji gdy biometria rozwija się w znaczącym tempie, wojna z terrorem spowodowała gwałtowny wzrost zarówno finansowania działań badawczych jak i realizacji. Po 11 września 2001 r. w Stanach Zjednoczonych techniki biometryczne, dostępne do użytku handlowego lub prawie w pełni gotowe do zastosowania, zostały określone jako klucz do wygrania tego nowego rodzaju wojny.⁷⁸ „US Patriot Act”, amerykańskie prawo ustanowione po zamachu z 11 września, o implikacjach wykraczających poza terytorium Stanów Zjednoczonych, ustanowiło szereg praktyk odnoszących się do sposobów zastosowania informacji biometrycznych, które umożliwiły prawie nieograniczone wykorzystanie ich przy prowadzeniu dochodzeń i działań związanych z identyfikacją terrorystów.

⁷⁶ Accenture Digital Forum (2004) „US Homeland Security to Develop and Implement program at air, land and sea ports of entry [Rozwój i realizacja programu bezpieczeństwa wewnętrznego Stanów Zjednoczonych w powietrzu, na lądzie i morskich portach wejścia]” <http://www.digitalforum.accenture.com>

⁷⁷ deGoede, M. (2003) „Hawala discourses and the war on terrorist finance [Wykłady na temat hawala i środków finansowych wojny z terroryzmem]”, *Environment and Planning D: Society and Space* 21(5): 513-532. Chalfin, B. (2004) „Border scans: sovereignty, surveillance and the customs service in Ghana [Skany graniczne: suwerenność, nadzór i służby celne w Ghana]”, *Identities: Global Studies in Culture and Power* 11: 397-416.

⁷⁸ Amoore, L. (2006) „Biometric borders: governing mobilities in the war on terror [Granice biometryczne: zarządzanie przemieszczaniem się podczas wojny z terroryzmem]”, *Political Geography* 25: 2: 336-351; Gates, K. (2005) „Biometrics and post-9/11 technostalgia [Biometria i technologie po dniu 11 września]”, *Social Text* 23(2): 35-53. Irma Van der Ploeg, „Biometrics and the body as information [Biometria i ciało jako źródło informacji]”, w Lyon, D. (wyd.) (2003) *op cit.* nr 6.

9.7.3. W brytyjskich miastach, takich jak Newham, Birmingham, Tameside, Manchester i innych, a także w Stanach Zjednoczonych po pierwszych doświadczeniach związanych z programami komputerowymi do rozpoznawania twarzy, zastosowanie cyfrowej telewizji CCTV, wykorzystującej algorytmy komputerowe do automatycznego szukania określonych osób lub zachowań nabiera rozmachu. Główne przeszkody techniczne, na jakie napotyka system do rozpoznawania twarzy czy inne systemy biometryczne CCTV, to te związane z funkcjonowaniem na zewnątrz, na ulicach miast. Jednak przeszkody te zostaną szybko zlikwidowane dzięki znaczącym nakładom na programy badawczo-rozwojowe.⁷⁹

9.8. Namierzanie, śledzenie i zakładanie lokalizatora

9.8.1. Geograficzne Systemy Informacyjne (GIS)⁸⁰ coraz częściej odnoszą się do praktyki nadzoru, organizują ją i pomagają w namierzaniu. W rzeczywistości wiele z nich śledzi przemieszczanie się ludzi, pojazdów lub towarów za pomocą chipów RFID, systemu GPS, chipowych dowodów tożsamości, transponderów lub sygnałów radiowych emitowanych przez telefony komórkowe lub przenośne komputery.

9.8.2. Zgodnie z cytowaną w raporcie BBC wypowiedzią specjalisty medycyny sądowej, dane pochodzące z łączności mobilnej mogą powiązać podejrzenia z przestępstwem: „jeśli dana osoba prowadzi rozmowę z telefonu komórkowego, i jest zamieszana w przestępstwo, istnieje możliwość określenia [na podstawie danych łączności mobilnej] miejsca wykonania połączenia telefonicznego na podstawie śladów radiowych”.⁸¹ Często nie ma rozróżnienia między elektronicznym urządzeniem przenośnym rozumianym właśnie jako urządzenie, a jego użytkownikiem. Zgodnie z brytyjskim Ministerstwem Spraw Wewnętrznych „dane dotyczące łączności są bardzo ważnym narzędziem śledczym, pozwalającym na ustalenie powiązań między osobami podejrzanymi (szczegółowy rachunek) lub ustalenie miejsca pobytu danej osoby w danym czasie, potwierdzając lub obalając alibi (analiza lokalizacji komórki)”.⁸²

9.8.3. Zarówno GPS, jak i RFID uważane są coraz częściej za rozwiązania w dziedzinie egzekwowania prawa i zarządzania personelem. Monitorowanie elektroniczne zostało także wprowadzone jako warunek wyrażenia zgody na zwolnienie za kaucją, a w 2004/05 około 631 osobom dorosłym i 5751 nieletnim, niektórym w wieku 12 lat założono lokalizator, pozwalając im tym samym na oczekiwanie rozprawy w domu, a nie w areszcie.⁸³ Także przestępcy wypuszczani z więzienia są często obiektem monitorowania elektronicznego, stosowanego albo w przypadku przedterminowego zwolnienia z zakładu

⁷⁹ Zob. Norris, C. (2003) „From personal to digital: CCTV, the panopticon, and the technological mediation of suspicion and social control [Od osobistego do cyfrowego: CCTV, panopticon technologiczne mediacje podejrzliwości i kontrola społeczeństwa]”, w Lyon, D. (wyd.) (2003) *op cit.* nr6; Norris, C. i Armstrong, G. 1999: *The Maximum Surveillance Society: The Rise of CCTV [Maksymalne społeczeństwo nadzoru: rozwój CCTV]*, Oxford: Berg.

⁸⁰ Institute for the Future (2004) *Infrastructure for the New Geography [Infrastruktura dla nowej geografii]*, Menlo Park, CA: IFTF.

⁸¹ „Phone firms ‘flooded’ by crime checks [Firmy telefoniczne zalane fałszywymi kontrolami]”. *BBC News*, 20 grudzień 2002, <http://news.bbc.co.uk/1/low/uk/2592707.stm>

⁸² Zob. Home Office (Ministerstwo Spraw Wewnętrznych Wielkiej Brytanii) (2006) *Surveillance: Access to Data [Nadzór: dostęp do danych]*, <http://security.homeoffice.gov.uk/surveillance/access-to-data/>

⁸³ NPS (National Probation Service - krajowe służby kuratorskie) (2006) *Electronic Monitoring 6 [Monitoring elektroniczny 6]*. <http://www.probation.homeoffice.gov.uk/output/Page137.asp#Current%20Programmes>.

karnego w ramach brytyjskiego programu „Home Detention Curfew Scheme”⁸⁴, albo w przypadku zwolnienia warunkowego.⁸⁵

- 9.8.4. RFID stanowi podstawę dla nowych inteligentnych środków bezprzewodowego śledzenia przemieszczania się towarów i ludzi. Chipy emitują ograniczony zakres sygnałów radiowych, które mogą zostać wychwycone przez odbiorniki na ogół z odległości kilku centymetrów. Inną istotną kwestią jest różnica między RFID aktywnym a pasywnym. Coraz częściej wykorzystywanie możliwości aktywnego RFID jest na porządku dziennym. W istocie, ostatnie interesujące oferty złożone w związku z zamówieniami rządowymi na zapewnienie bezpieczeństwa granic uwzględniały demonstrację możliwości bezprzewodowych urządzeń namierzających.
- 9.8.5. Do niedawna ich zastosowanie ograniczało się do dużych kontenerów transportowych, towarów konsumpcyjnych i różnych rodzajów kart chipowych. W Stanach Zjednoczonych mimo sformułowania poważnych zarzutów przeciwko propozycjom wprowadzenia RFID w paszportach i wizach, karty chipowe RFID były testowane na granicy amerykańsko-meksykańskiej. Po stronie podaży, przemysł RFID sygnalizuje możliwości technologii pozwalające na śledzenie i obserwowanie pracowników-migrantów, którzy przekraczają granicę w określonym okresie.
- 9.8.6. Ostatnio miała miejsce godna uwagi, w dużej mierze niezauważona zmiana: wszczepianie urządzeń istotom żyjącym. Początkowo chipowanie przeprowadzane było tylko u koni wyścigowych, następnie stosowanie mikrochipów zawierających informacje o szczepieniach i właścicielach stopniowo zastąpiło unijne wymogi kwarantanny dla zwierząt domowych w programie PETS stosowanym od 28 lutego 2000; program ten rozszerzono już poza Europę⁸⁶.
- 9.8.7. Chipy RFID u ludzi po raz pierwszy zostały zastosowane w Stanach Zjednoczonych w stosunku do osób starszych cierpiących na choroby degeneracyjne. Około 70 osobom cierpiącym na degeneracyjne choroby mózgu wszczepiono chipy umożliwiające ich opiekunom łatwe ustalenie ich miejsca przebywania⁸⁷. Naukowcy i entuzjaści technologiczni przez kilka lat sami sobie wszczepiali chipy⁸⁸, a ostatnio sieć hiszpańskich klubów nocnych zaproponowała swoim stałym klientom możliwość zapisania na wszczepionych chipach pewnych informacji na temat przywilejów finansowych i związanych z wejściem do klubu⁸⁹. Natomiast kolejny krok miał miejsce w lutym 2006 r., kiedy firma ochroniarska w Ohio w Stanach Zjednoczonych wszczepiła 2 swoim pracownikom chipy RFID umożliwiając im w ten sposób wejście na teren firmy⁹⁰. Pomimo bardzo inwazyjnego charakteru tej procedury została ona przeprowadzona dobrowolnie, w konsekwencji czego należałoby się zastanowić

⁸⁴ System HDC umożliwia zwolnienie osób skazanych na pobyt w więzieniu od 3 miesięcy do mniej niż 4 lata od 2 tygodni do czterech i pół miesiąca wcześniej, pod warunkiem że prowadzony będzie elektroniczny monitoring tychże osób. W 2004/05 19096 osób zostało zwolnionych w ramach programu (*ibid.*: 6).

⁸⁵ NPS *op cit.*

⁸⁶ W celu uzyskania szczegółowych informacji zob.: DEFRA (Department of Environment, Food and Rural Affairs – Brytyjski Departament Środowiska, Żywności i Obszarów Wiejskich) (2006) Pet Travel Scheme [program przewozu zwierząt], <http://www.defra.gov.uk/animalh/quarantine/pets/index.htm>

⁸⁷ Zaangażowaną firmą jest Verichip Corporation. <http://www.verichipcorp.com/>.

⁸⁸ Amal Graafstra jest jednym ze zwolenników samochipowania się. Objasnienia, obrazy i filmy można ściągnąć ze strony <http://amal.net/rfid.html>.

⁸⁹ Graham-Rowe, D. (2004) „Clubbers chose chip implants to jump queues [Klubowicze decydują się na zakładanie chipów aby omijać kolejki]”, *New Scientist*, 21 May, <http://www.newscientist.com/article.ns?id=dn5022>.

⁹⁰ Waters, R. (2006) „US group implants electronic tags in workers [Amerykańska grupa zakłada elektroniczne tagi pracownikom]”, *Financial Times*, 12 February. <http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html>.

nad tak ważną kwestią, jak integralność ciała i prywatności w odniesieniu do pracowników. Nie dziwi zatem, że koncepcja wzywająca wszystkich do poddania się wszczepianiu chipów stanowi obecnie temat poważnych dyskusji na niektórych portalach technologicznych.

9.8.8. Z komercyjnego punktu widzenia, zarówno tagi RFID, jak i GPS są postrzegane przez firmy jako możliwość świadczenia usług marketingowych ściśle dostosowanych do potrzeb klientów, oferując na przykład zniżki na urządzenia przenośne punktom sprzedaży detalicznej znajdującym się w danym miejscu. Jednakże wykorzystywanie urządzeń zarówno RFID, jak i GPS jest utrudnione ze względu na koszty technologii ich wykonania, które mogą przewyższać wartość produktu, do którego są przymocowane. Ich zastosowanie zależało w dużym stopniu od zarządzania personelem i towarem, czyli form nadzorowania miejsca pracy, a w związku z tym, że tego typu technologie stają się coraz tańsze, urządzenia służące do określania położenia, w szczególności chipy RFID, prawdopodobnie będą wykorzystywane do monitorowania zarówno produktów jak i samych konsumentów.⁹¹ Ciągły rozwój w kontekście stosowania danych geograficznych uzyskiwanych w rzeczywistym czasie w odniesieniu do profili konsumentów dostarczy kolejnych informacji umożliwiających skuteczniejsze kierowanie kampanii reklamowych do konkretnych konsumentów. Funkcje tych technologii mają duże szanse na "rozrost".

9.9. Synergia technologiczna i zmiana celu

9.9.1. Podczas gdy możliwości poszczególnych technologii i systemów mają duże znaczenie, nie należy zapominać o rosnącej synergii technologicznej, czy konwergencji technologii związanych z nadzorem. Tendencja, ta mająca charakter długoterminowy w kontekście systemów komputerowych, jest motywowana także chęcią osiągnięcia ekonomii skali. Coraz więcej systemów jest projektowanych z myślą o ich interoperacyjności. Oznacza to również, że skutkiem stosowania starszych technologii, które ustawodawcy rozumieli i którymi zarządzali, mogą być nowe produkty, które będą funkcjonować w sposób nieprzewidywalny i nieuregulowany.

9.9.2. Interoperacyjność i synergia technologiczna mogą zostać dodane do prostszej ale powszechnej "zmiany celu" ponieważ liczba zainteresowanych użytkowników rośnie, a informacje gromadzone w jednym konkretnym celu lub na temat danej dziedziny mogą przechodzić na potrzeby innych. Na przykład, nie tylko takie same są techniki eksploracji danych, opracowane na potrzeby profilowania konsumentów oraz techniki stosowane przez firmy ochroniarskie czy służby wywiadowcze do określania potencjalnych terrorystów, ale także często właśnie te dane, na podstawie których takie profile są tworzone są takie same. Istnieją też obecnie pewne dowody, że dominacja konkretnej firmy w zastosowaniu handlowym technologii (na przykład wejściowe systemy ochrony opierające się na odciskach palców wprowadzone dla zapewnienia bezpieczeństwa miejsca pracy) jest kluczowym czynnikiem ich sukcesów w procesie zapewniania bezpieczeństwa. W miejscach pracy technologie monitorowania pracowników mogą czasem dostarczyć więcej informacji niż planowano, a kierownictwo jest kuszone ideą rozszerzenia monitoringu bez skonsultowania tego z pracownikami. Może to mieć duże znaczenie w sytuacji,

⁹¹ Zob. Lyon, D., Marmura, S. i Peroff, P. (2005) *Location Technologies: Mobility, Surveillance and Privacy [technologie lokalizacji: mobilność, nadzór i prywatność]*, Queens University, Kingston, Ontario: The Surveillance Project [Projekt Nadzoru]. <http://www.queensu.ca/sociology/Surveillance/files/loctech.pdf>.

gdy informacje są wykorzystywane do podejmowania decyzji na temat wynagrodzenia czy awansów.

9.9.3. Obecnie kładzie się nacisk na stworzenie takich identyfikatorów, które mogłoby być wykorzystywane do różnych celów, jak na przykład przy przekraczaniu granicy, do kontrolowania oszustw, dostępu do informacji rządowych czy handlowych (wypożyczalnia kaset wideo), jak również tych o charakterze częściowo handlowym (biblioteki); nacisk ten wywiera wpływ na kształtowanie całości zagadnienia. Kluczowym problemem jest to, że po zainstalowaniu takich systemów mogą one w łatwy sposób zacząć żyć własnym życiem, przy czym wprowadzenie systemu jest znacznie łatwiejsze niż zatrzymanie go lub zmienienie jego kierunku. W sytuacji gdy programy takie jak „wojna z terroryzmem”, powstrzymanie migracji niepożądanych grup, a także poszukiwanie rozwiązania pozwalającego na walkę z oszustwami za pomocą kart kredytowych kształtują rozwój systemów identyfikacji tożsamości, etos klasycznej biurokracji wydaje się być osłabiony. Największa trudność leży w uprawnieniach przyznanych państwu (oraz firmom i organom technicznym) kontrolującemu środki służące do identyfikacji.

9.9.4. Kolejnym przykładem może być londyński system do kontrolowania ruchu ulicznego, który służył początkowo jako narzędzie przeciwko atakom terrorystycznym, a obecnie wykorzystywany jest do poszukiwania podejrzanych i skradzionych pojazdów. Historia ANPR w Londynie pokazuje również, że zmiana celu może mieć miejsce na kilka sposobów: początkowym przeznaczeniem tego systemu było przeznaczenie militarne, miał on służyć do identyfikacji terrorystów IRA. Obecnie służy zarządzaniu ruchem ulicznym, ochronie przed nowym pokoleniem terrorystów, a także zwiększaniu dochodów administracji lokalnej.

9.9.5. W przypadku nadzoru medycznego, wykorzystanie technologii służących nadzorowi diagnostycznemu może być znacznie szersze, i może odnosić się do coraz większych części społeczeństwa. W szczególności odnotowywana została tendencja do zmiany celu na cele medycyny sądowej. Wiele technologii wykorzystywanych na potrzeby diagnostyki medycznej znalazło zastosowanie w medycynie sądowej. Przykładem mogą być analizy DNA wycinków tkanki, analizy cech charakterystycznych związanych z ciałem, takich jak postawa, chód czy wyraz twarzy, analizy dotyczące części ciała, obrazów lub odcisków (na przykład odciski palców, wzrost, waga, proporcje ciała). Wiele z nich proponowanych jest obecnie dla potrzeb nadzoru w formie rozległych baz danych, na podstawie których można sprawdzić tożsamość.

9.9.6. Dzięki przepływowi i przekazywaniu danych, organizacje mają pełną możliwość gromadzenia, przechowywania i manipulowania danymi (i aktualnie są zobligowane przez prawo do przechowywania ich przez dłuższy czas). Pozwala to wyraźnie na zmianę celu w kontekście nadzoru danych telekomunikacyjnych, a tam, gdzie jest duży udział państwa i sektorów korporacyjnych, osoby, których dane dotyczą mają niewielki wpływ na sposób, w jaki ich dane są gromadzone, przechowywane, udostępniane, kupowane czy sprzedawane.

9.10. *W kierunku wszechobecnego nadzoru*

9.10.1. Znaczenie technologii nabiera powagi, gdy stają się one wszechobecne, uznawane za coś oczywistego i gdy w znacznym stopniu są niewidoczne. Zgodnie z myślą Marka Weinera wypowiedzianą w 1991 r. "najgłębsze

technologie to te, które znikają. Wplatają się w tkaninę codziennego życia dotąd, aż stają się nie do odróżnienia”.⁹² Cyfrowa, połączona w sieci technologia nadzoru zmierza w kierunku wszechobecności. Przetwarzanie bez granic (ang. *pervasive* lub *ubiquitous computing*) (Ubicomp), w Europie znane jako inteligentne otoczenie (AmI), stwarza warunki do powstania wszechobecnego nadzoru.⁹³ Jedną z zasadniczych kwestii dotyczących Ubicomp jest koncepcja Uniform Resource Locator (URL) (jednolity lokalizator zasobów), znana większości dzięki korzystaniu z adresów internetowych. Jakkolwiek URL był zawsze uważany za coś więcej. Uważa się, że jest w stanie dostarczyć informacji o miejscu w sieci wszystkich przedmiotów i ludzi.

9.10.2. Takie ciągle sortowanie ludzi i ich szans życiowych w miastach za pomocą programów komputerowych jest organizowane za pomocą mnóstwa urządzeń elektronicznych i fizycznych „punktów przejścia” czy „przewężeń” pokonywanych za pomocą zwiększającej się liczby słów kodowych, haseł, numerów PIN, nazw użytkownika, kontroli dostępu, kart elektronicznych czy skanów biometrycznych. Niektóre są dobrze widoczne i chętnie akceptowane (zakupy dokonywane za pomocą karty kredytowej wymagającej użycia kodu PIN lub kontrola paszportowa na lotnisku). Inne są bardziej ukryte (korzystanie z Internetu czy telefonicznych centrów obsługi klienta). W innych przypadkach punkt przejścia jest wyraźny (kamera CCTV na ulicy lub kamera rejestrująca prędkość na autostradzie), jednak nie można być pewnym czy czyjaś twarz czy też tablica rejestracyjna samochodu rzeczywiście zostały zeskanowane.

9.10.3. Usługi elektroniczne i podobne dziedziny są stosunkowo łatwe do kontrolowania w porównaniu z ulicami miast, jednak coraz więcej punktów przejścia kontrolowanych jest za pomocą urządzeń elektronicznych i fizycznych blisko ze sobą współpracujących. Połączenie CCTV, informacji biometrycznych i technologii śledzenia może być postrzegane jako część znacznie szerszego zastosowania, często finansowanego ze środków, jakie Zjednoczone Królestwo / Stany Zjednoczone przeznaczają na wojnę z terroryzmem, wykorzystania powiązanych ze sobą inteligentnych systemów służących do śledzenia przemieszczania się i zachowań milionów ludzi zarówno w czasie, jak i przestrzeni. W branżowym żargonie takie zjawisko nosi nazwę wieloskalowego czasowo-przestrzennego śledzenia.⁹⁴

9.11. Ograniczenia technologiczne

9.11.1. Oczywiście technologie nie spełniają w pełni oczekiwań, jakie z nimi są związane. Na przykład w przypadku technologii biometrycznych stworzonych dla potrzeb programu USVISIT, planowane skanowanie tęczówki z powodów logistycznych zostało zastąpione identyfikacją za pomocą cyfrowych odcisków palców. Podobnie było w przypadku elementów biometrycznych brytyjskiego programu e-Borders, których wdrożenie napotkało na trudności. W związku z tym, elementy biometryczne odnoszące się do praktyk rutynowego nadzoru granicznego są stosunkowo słabo rozwinięte.

⁹² Weiner, M. (1991) „The computer for the 21st century[Komputer XXI wieku]”, *Scientific American*, 265 (September): 94-104.

⁹³ Kang, J. i Cuff, D. (2005), *Pervasive Computing: Embedded in the Public Sphere* [Przetwarzanie bez granic e sferze życia publicznego], dostępne na dcuff@ucla.edu. Cuff, D. (2002) Immanent domain: Pervasive computing and the public realm [Immanentna dziedzina: przetwarzanie bez granic i sfera publiczna], *Journal of Architectural Education*, 57: 43-49.

⁹⁴ Hampapur, A. et al. (2005), „Smart video surveillance [Inteligentny nadzór za pomocą kamer wideo]”, *IEEE Signal Processing Magazine*, marzec: 38-51.

9.11.2. Niektóre z tych problemów dotyczą wiarygodności⁹⁵, przy czym wyróżniającymi się problemami są te dotyczące „nieudanego zapisu” („failure to enrol”, FTE) (informacja biometryczna jest nierozpoznawalna) i informacji „false non-match” oznaczającej, że dane nie pasują (kolejny odczyt nie pasuje do zapisanej właściwości biometrycznej danej osoby). Mimo to główne decyzje dotyczące wdrażania są na ogół podejmowane przed pojawieniem się problemów. Na przykład w przypadku proponowanego brytyjskiego systemu identyfikacji tożsamości oszacowano, że jedna osoba na sześć może nie mieć możliwości wykorzystania swojego dowodu tożsamości właśnie z powodu problemów FTE.⁹⁶

9.11.3. To, czy diagnostyka medyczna, medycyna sądowa czy inna technika nadzoru pociągająca za sobą problematyczną i/lub predyktywną identyfikację celów powoduje powstanie „false non-match” zależy od dwóch ważnych elementów: *czułości* i *specyficzności* wykorzystywanej technologii. **Czułość** jest to zdolność technologii do identyfikowania istotnych przypadków w sposób poprawny. **Specyficzność** (znana również jako **selektywność**) jest to zdolność technologii do wykluczenia nieistotnych przypadków w sposób poprawny. Indywidualne cechy charakterystyczne, ustawienia organizacyjne, kryteria testowe i wiedza związana z daną dziedziną dadzą różne wyniki związane z czułością i specyficznością. Wartości wskaźników czułości i specyficzności zależą także od kryteriów testowych (na przykład skany ultradźwiękowe płodu w kierunku syndromu Downa przeprowadzane są przez osobę wykwalifikowaną lub częściowo wykwalifikowaną) i działają na zasadzie wymiany. Zwiększająca się czułość oznacza identyfikację większej liczby potencjalnych celów, ale (koniecznie) w obrębie zidentyfikowanej populacji większa będzie liczba celów zidentyfikowanych wątpliwie i błędnie, tak więc selektywność spada. Dlatego żaden test nie jest doskonały, a ustalenie wartości progowej czułości/specyficzności jest w takim samym stopniu wynikiem czynników politycznych, społecznych i organizacyjnych, co w przypadku technologii. W związku z powyższym należy przyjąć, że pewien odsetek zidentyfikowanej populacji będzie wynikiem fałszywie negatywnym lub fałszywie pozytywnym. Z tego powodu należy rozważyć więcej wartości: *pozytywna i negatywna wartość predyktywna* testu. Pozytywna wartość predyktywna jest odsetkiem wyników prawdziwie pozytywnych spośród wszystkich pozytywnych wyników testu i odpowiednio negatywna wartość predyktywna jest odsetkiem wyników prawdziwie negatywnych spośród wszystkich negatywnych wyników testu. Wartości predyktywne testu zależą od dokładności wskaźników, na których test się opiera.

9.11.4. Jako że gromadzenie danych osobowych stwarza odpowiednie warunki do pojawienia się nadzoru predyktywnego, uprzedzającego i prewencyjnego w szerszym zakresie ustawień, niedoskonałości metod statystycznych mogą mieć daleko idące konsekwencje w odniesieniu do danych, które zostały fałszywie zidentyfikowane. Błędy tego typu mogą mieć większe znaczenie niż ograniczenie dostępu do miejsc lub usług: w przypadku nadzoru medycznego, mogą stanowić zagrożenie dla życia, a ich powszechność jest dużo większa niż się wydaje. W rzeczywistości jedynie najnowsze formy technologii biometrycznych, takie jak typowanie DNA i rozpoznawanie twarzy, zostały poddane testom, których wyniki dostarczają nam podstaw do przeprowadzenia szacunkowych obliczeń współczynników błędu, a metodologie używane do oszacowania wskaźników błędu są mniej precyzyjne niż te, które są używane

⁹⁵ Zob. Zureik, E. i Hindle, K. (2004) „Governance, security and technology: the case of biometrics [Rządy, bezpieczeństwo i technologia: przypadek biometrii]” *Studies in Political Economy*, 73: 113-137.

⁹⁶ Zob. Grayling, A.C. (2005) *In Freedom's Name: The Case Against Identity Cards [W imię wolności: Sprawa przeciwko dowodom tożsamości]*, London: Liberty.

dla potrzeb technologii medycznych. Najlepszy system zbadany w 2004 r. za pomocą testów amerykańskich sił wojskowych służących do rozpoznawania twarzy ludzkiej, Facial Recognition Vendor Tests (FRVT), uzyskał wskaźnik identyfikacji wynoszący zaledwie 74% w idealnych warunkach, przy czym należy zauważyć, że ten test nie badał bardziej złożonych przypadków występowania poszukiwanej twarzy w obrębie danej populacji. Rozpoznanie twarzy ludzkiej w realistycznych okolicznościach nie zapewnia żadnego wiarygodnego bezpieczeństwa nawet w przypadku znanych terrorystów.

9.11.5. Jeśli chodzi o DNA, nawet w sądach założono, że identyfikacja DNA jest nieomylna. Jednakże dla potrzeb identyfikacji medycyny sądowej badaniom poddaje się jedynie kilka małych segmentów całego łańcucha DNA i tylko serie repetytywnych sekwencji (tak zwanych „stutterów”) w ramach tak zwanych śmieciowych DNA są przedstawiane w tak zwanym profilu. Jednakże podczas gdy negatywne testy DNA wydają się być prawie doskonałym narzędziem do uniewinnienia osoby niewinnej, rzadko występujące wyniki fałszywie negatywne, zaskakująco prawdopodobne wyniki fałszywie pozytywne i pozytywne testy DNA mogą się spotkać ze znacznie większym sceptycyzmem niż ma to na ogół miejsce w sądach.

9.11.6. Nawet o wiele mniej skomplikowane technologie do rozpoznawania, takie jak systemy ANPR, nie mają 100% dokładności w odczytywaniu szczegółów tablicy rejestracyjnej⁹⁷ pojazdu, co nieuchronnie oznacza, że informacje znajdujące się w bazie danych będą zagrożone, oraz że system może doprowadzić do pojazdu osoby mylnie zidentyfikowanej jako osoba powiązana ze znanymi przestępcami. Kwestia błędnej identyfikacji na podstawie policyjnych baz danych została ostatnio ujawniona w sytuacji gdy brytyjski rejestr karny (Criminal Records Bureau) wykazał, że około 2 700 osób zostało błędnie zidentyfikowanych jako osoby skazane za przestępstwa kryminalne. W wyniku błędnych informacji zawartych w ich danych, wielu z nich odmówiono przyjęcia do pracy. Problem związany z jakością danych przechowywanych w państwowym komputerowym systemie policyjnym był podkreślany w wielu raportach inspektoratu policyjnego;⁹⁸ w ostatnim raporcie zwrócono uwagę, że 22% danych w państwowym komputerowym systemie policyjnym nadal zawiera błędy, mimo kontroli inspektora.⁹⁹ Perspektywa wykorzystania bazy danych niesie również ze sobą ryzyko, ponieważ niskiej jakości dane wywiadowcze pochodzące z niepewnego źródła są coraz powszechniej udostępniane i wykorzystywane jako podstawa opartych na ryzyku procesów decyzyjnych różnych agencji.

9.12. „Zamknięcie” technologiczne i opóźnienie regulacyjne

9.12.1. Awaria lub niewystarczalność technologiczna mogą zatem doprowadzić do uzyskania gorszych wyników w zakresie szans życiowych niż w przypadku sprawnie działającego systemu technologicznego. Jednak nie można użyć tego argumentu, ponieważ wówczas wystarczyłoby odpowiedzieć po prostu „należy wykorzystać lepsze technologie”. Nadzór, pierwsze nasuwające się rozwiązanie

⁹⁷ PA Consulting (2004) *op. cit.* nr 51, sugeruje że dokładność odczytu wynosi około 96%, co może wydawać się wysokim wynikiem, niemniej jednak nawet jeśli jeden procent tablic rejestracyjnych zostanie błędnie odczytany i zarejestrowanych w bazie danych, może to potencjalnie podnieść liczbę dziennie rejestrowanych błędnie tablic do pół miliona.

⁹⁸ Zob. na przykład HMI Constabulary (2002) *Police National Computer: Data Quality and Timeliness, Second Report [Państwowy komputerowy system policyjny: jakość danych i odpowiedni czas, Drugi raport]*, London: HMI Constabulary.

⁹⁹ HMI Constabulary (2006) *Police National Computer Compliance Report: Avon and Somerset Constabulary [Raport na temat zgodności państwowego komputerowego systemu policyjnego policji w Avon i Somerset]*, str.16, par. 2.5.1 http://inspectorates.homeoffice.gov.uk/hmic/inspect_reports1/pnc-audits.html/a-and-s-pnc06.pdf?view=Binary

każdego rodzaju problemu, jest silnie związany ze szczeblem kierowniczym; doradcy do spraw zarządzania, którzy operują panującymi na świecie poglądami opartymi na pomiarach, często proponują nadzór rządowi. Dlatego też zaczęto bez problemów promować technologie nadzoru jako „odповідź” na liczne zagrożenia, a ostatnio na zagrożenie terroryzmem. Na przykład pewna gazeta amerykańska prezentująca konserwatywne poglądy opowiedziała się za zagęszczoną infrastrukturą miejską zautomatyzowanych systemów softwarowych i mikroczujników: „Rozmieszczone wzdłuż poboczy, wzniesień i szlaków, będą dostarczały informacje o wszystkim, co może nas zainteresować – o przejeżdżających pojazdach, woni materiałów wybuchowych, rozmowach pieszych, wyglądzie, brzmieniu, wadze, temperaturze, a nawet zapachu niemal każdego obiektu”¹⁰⁰.

9.12.2. Jednak im bardziej państwa, organizacje, wspólnoty i ludzie uzależnią się od technologii nadzoru, tym częściej mamy do czynienia z wyraźnym „zamknięciem” uniemożliwiającym rozważenie innych rozwiązań, a także z luką w rozumieniu, która zwiększa zależność od wiedzy spoza systemu demokratycznego. Dowody tożsamości są kluczowe dla sprawy i nieuchronnie będą zwiększały nasze uzależnienie od osób, które dostarczają ekspertyzy zarówno technologiczne jak i handlowe. Podczas gdy większość polityk obejmuje obecnie technologiczne komponenty, organy nadzorujące wciąż są w tyle za innowacjami technologicznymi i nie są w stanie pojąć, „jak to działa”. Istnieje zatem znaczne opóźnienie regulacyjne wynikające z braku wiedzy i zrozumienia rozwoju technologicznego. W tym nieustającym pościgu trzeba postawić pytanie, czy państwa są wyposażone w narzędzia niezbędne do wywiązania się z konkretnych regulacji dotyczących coraz bardziej skomplikowanych technologii i praktyk nadzoru. Pytanie, które często rodzi się przy okazji każdego rozwoju technologicznego, brzmi następująco: „Czy dzina można zamknąć z powrotem w butelce?”. Posiadacze i sprzedawcy patentów milczą, kiedy chodzi o odwracalność urządzeń i systemów.

10. Procesy nadzoru

10.1. Na funkcjonowanie społeczeństwa nadzorowanego składa się kilka kluczowych procesów. Jak już widzieliśmy, jednym z najbardziej istotnych elementów rozwoju jest sposób, w jaki nadzór, dawniej zarezerwowany dla „podejrzanych” lub „dewiantów”, objął większość ludności, którą można dzięki temu selekcjonować, klasyfikować i namierzać.

10.2. *Selekcja, klasyfikacja i namierzanie społeczne*

10.2.1. Selekcję społeczną można zaobserwować w wielu dziedzinach: i tak na przykład w trakcie dokonywania zakupów konsumenci nieustannie dostarczają sektorowi handlowemu dane konsumpcyjne, są częścią tworzącego się sprzężenia zwrotnego, które łączy działania konsumpcyjne z gromadzeniem danych umożliwiających przeprowadzenie transakcji.¹⁰¹ Konsumenci zaczęli oczekiwać, że przy okazji transakcji gospodarczych będą od nich wymagane formularze zawierające dane osobowe. Co więcej, często są nagradzani za przekazanie danych osobowych (na przykład, kiedy korzystają z programów lojalnościowych), ale poza tym nie wierzą, że nadzór konsumencki ma jakikolwiek wpływ na ich codzienne życie. A mimo to w procesie tym

¹⁰⁰ Huber, P.W. i M.P. Mills (2002) „How technology will defeat terrorism [W jaki sposób technologia pokona terroryzm]”, *City Journal* 12(1) http://www.city-journal.org/html/12_1_how_tech.html

¹⁰¹ Wyszczególniono w: Elmer, G. (2004) *op cit.* n.56.

konsumenci są włączani do systemu, który utrzymuje i wzmacnia systemy stratyfikacji, tworząc kategorie w oparciu o ich udział.

- 10.2.2. W miejscu pracy najlepszym przykładem jest sektor informacji telefonicznej. Punkty informacji telefonicznej tworzą rankingi rachunków klientów pod kątem ich wydatków. Im wyższe są wydatki, tym większa jest wartość klienta dla organizacji i dlatego, kiedy klienci, którzy płacą najwięcej, dzwonią do punktów informacyjnych, krócej oczekują na połączenie i są łączeni z bardziej wykwalifikowanymi pracownikami. Ponadto profil klienta jest postrzegany jako element decydujący przy rekrutowaniu pracowników punktów informacji telefonicznej, którzy są obecnie oceniani pod kątem kompetencji społecznych i znajomości obyczajów, dopasowanych do właściwości tego segmentu rynku, który obsługują.
- 10.2.3. Przedsiębiorstwa telekomunikacyjne (operatorzy sieci, operatorzy świadczący usługi internetowe, operatorzy udzielający informacji) rutynowo gromadzą i przetwarzają dane osobowe na temat swoich klientów w podobny sposób, w jaki czynią to inne organizacje sektora prywatnego, aby sortować i klasyfikować klientów jako konsumentów. Ponadto dla sektora prywatnego ważne jest dokonywanie rozróżnienia na zastrzeżone dane (osobowe) dotyczące naliczania opłat i na całkowicie archwizowalne dane dotyczące ruchu, zwłaszcza przy okazji kampanii marketingowych, takich jak te prowadzone za pomocą SMSów (krótkich wiadomości tekstowych).¹⁰²
- 10.2.4. Telefon komórkowy jest postrzegany przez konsumentów i sektor telekomunikacji jako osobiste urządzenie komunikacyjne, a możliwość komunikowania się z użytkownikami powoduje, że dane te mają wartość handlową. Jednocześnie numer telefonu komórkowego jako wskaźnik jest uznawany za anonimowy element informacji. Wskaźnik jest jednak wystarczająco precyzyjny, aby umożliwić technikom eksploracji danych odnajdywanie danych osobowych z danych, które powinny być anonimowe. Dlatego też nadzór telekomunikacyjny jednostek korporacyjnych potencjalnie sortuje konsumentów według ich wartości gospodarczej i może tego dokonać na podstawie nieuregulowanych danych na temat przekazywania, jak również danych dotyczących naliczania, chronionych ustawą o ochronie danych.
- 10.2.5. Atmosfera wzmożonych obaw o bezpieczeństwo narodowe nasila także pęd do „selekcji społecznej” na granicach kraju.¹⁰³ W sytuacji, gdy ktoś może zweryfikować swoją tożsamość i poświadczyć swoje działania, zapewne jego doświadczenie w przekraczaniu granic jest takie, że podróż przebiega sprawnie. Oczywiście trzeba pójść na kompromis, przedstawiając dane osobowe i biometryczne i umożliwiając dostęp do prywatnych informacji. W wielu lotniczych, morskich i drogowych przejściach granicznych bardzo często spotyka się na przykład drogi „szybkiego ruchu” przeznaczone do szybkiej odprawy, na przykład w przypadku systemu „Privum” na lotnisku Schiphol w Holandii, który wykorzystuje identyfikację tożsamości na podstawie obrazu tęczówki i pozwala uniknąć wyczekiwania w długich kolejkach do odprawy paszportowej. Takie uprzywatnione miejsca funkcjonowania systemu „trusted traveler” (zaufany podróżnik) mimo wszystko rodzą pytania na temat ochrony danych i prywatności. Ponadto coraz większa liczba strażników granicznych

¹⁰² Green, N i Smith, S. (2003) „'A spy in your pocket?' the regulation of mobile data in the UK [„Szpieg w twojej kieszeni?” kontrola danych na temat sieci bezprzewodowej w Zjednoczonym Królestwie]” *Surveillance & Society* 1(4): 573-587.
<http://www.suveillance-and-society.org/articles/v1i4/pocketspy.pdf>.

¹⁰³ Lyon, D. (2003) *op cit.* n.7; Lyon, D (ed.) (2003), *op cit.* n.6.

wyszkolonych w szybkiej odprawie selekcjonuje ludzi i transakcje na kategorie pod kątem ryzyka, co umożliwia większy nadzór nad tymi, którzy nie mają wstępu lub nie mogą wkraczać na tereny prywatne.

- 10.2.6. Ostatecznie zaproponowany w Zjednoczonym Królestwie system identyfikacji tożsamości miałby możliwość selekcjonowania ludzi na tych, którzy mogą mieć dostęp i na innych. Będą działać także niewidoczne mechanizmy, kierujące system przeciwko tym, którzy prawdopodobnie znajdują się już w niekorzystnej sytuacji. To właśnie ta umiejętność dokonywania selekcji społecznej może w dłuższej perspektywie stać się jeszcze bardziej zdradliwa, niż wywołująca obawy ograniczona możliwość poruszania się w krajach, w których policja może w każdej chwili zażądać okazania dokumentów tożsamości.¹⁰⁴ Taka selekcja społeczna prowadzi do utworzenia obywatelstwa drugiej kategorii, zamiast wspierać bardziej solidarystyczną i egalitarną praktykę.
- 10.2.7. Klasyfikowanie wiąże się z selekcjonowaniem ludności na kategorie, a następnie z dokonywaniem podziału klasowego w ramach tych kategorii i pomiędzy nimi. Ma to miejsce w sercu najbardziej naukowej praktyki zarządzania¹⁰⁵. A państwa i instytucje korzystały przecież z takich systemów przez wiele lat, przy czym ich działania obejmowały zarówno egzaminy i stopnie, jak i nakładanie na więźniów, żołnierzy i innych obowiązku noszenia rozpoznawalnej odzieży (uniformów), a w ekstremalnych przypadkach, tak jak w hitlerowskich Niemczech, obowiązku noszenia na ubraniach oznaczeń przyporządkowanych kategoriom, takich jak żółta gwiazda dla Żydów, i tatuowania numerów na skórze więźniów obozów koncentracyjnych.
- 10.2.8. Jedną z najważniejszych kategorii dla państwa jest kategoria obywatelstwa. Obywatelstwo i nadzór mają swoje miejsce we współczesnym świecie. Obszerne akta na temat każdej osoby są potrzebne, aby informować organy administracji rządowej na temat tego, kto ma do czego prawo.
- 10.2.9. Od końca dwudziestego wieku większość tych akt była wprowadzana do systemów komputerowych i coraz częściej są one łączone i automatyzowane. Początek dwudziestego pierwszego wieku to rozwój kilku nowych krajowych systemów identyfikacji. W marcu 2006 r. Zjednoczone Królestwo zatwierdziło w parlamencie plany w odpowiedzi na wydarzenia z 11 września i „wojnę z terroryzmem”. Identyfikacja obywatelska nie bazuje wyłącznie na dowodach tożsamości. Nowe krajowe systemy wykorzystujące dowody tożsamości opierają się na rejestrze krajowym, bazie danych (lub bazach danych w przypadku Zjednoczonego Królestwa) zawierającej informacje osobowe, które można przeszukiwać i sprawdzać niezależnie od wszelkich żądań okazania dowodu będącego w posiadaniu obywatela. Niepowtarzalny identyfikator wbudowany w kartę jest także kluczem odblokowującym bazę(y) danych, a zatem jako taki stanowi źródło znacznej władzy.¹⁰⁶ Umożliwia dostęp do kilku rodzajów baz danych; im bardziej uniwersalny jest system, tym więcej baz danych może być zaangażowanych. W sytuacji, gdy system Zjednoczonego Królestwa wykorzystujący dowody tożsamości ma bronić przed „kradzieżą tożsamości”, i tak dostępne będą dane handlowe, podobnie jak dane rządowe.

¹⁰⁴ Lyon, D. (2004) *ID Cards: Social Sorting by Database [Dowody tożsamości: Selekcja społeczna na podstawie bazy danych]*, OII Issue Brief 2004; Oxford: Oxford Internet Institute.

¹⁰⁵ Bowker, G. i Star, S. L. (1999) *Sorting it Out: Classification and its Consequences* [Selekcja: klasyfikacja i jej konsekwencje], Cambridge MA: MIT Press.

¹⁰⁶ Zob. np.: Clarke, R. (2006) „National Identity Schemes: The Elements [Krajowe systemy identyfikacji: elementy składowe]” <http://www.anu.edu.au/people/Roger.Clarke/DV/NatIDSchemeElms.html>

10.2.10. Po drugie, tereny publiczne oraz fizyczne i elektroniczne infrastruktury miast są szybko restrukturyzowane w sposób, który bezpośrednio wykorzystuje możliwości nowych technologii nadzoru. Coraz rzadziej stosuje się uniwersalne i znormalizowane przepisy dotyczące dostępu do usług, terenów i infrastruktury, oparte na pojęciach demokratycznego obywatelstwa i otwartego dostępu lub tradycyjnych ideach usług i terenów publicznych, do których mają wolny dostęp wszyscy w momencie działań konsumpcyjnych lub do których dostęp jest odpłatny według uniwersalnych taryf. Coraz częściej z kolei wykorzystywane są pojęcia ukierunkowanych usług, infrastruktury i terenów, dostępnych jedynie dla osób upoważnionych i wycenianych bardzo różnie dla różnych osób i różnych miejsc.

10.2.11. Profile dostarczają przedsiębiorstwom środki, które pozwalają im skierować swoją strategię marketingową do węższej grupy konsumentów, obniżając przy tym koszty marketingowe i zwiększając wskaźniki odpowiedzi. Często jest to dużo tańsze od masowych kanałów marketingowych w telewizji czy radiu i reklam drukowanych. Na przykład bank, który podpisał umowę z biurem podróży, może sprzedawać wakacyjne wyjazdy rodzinne tym, których zaklasyfikował jako rodziny, oferując inny zestaw ofert podróży tym, którzy są na emeryturze.¹⁰⁷ Sprzedawcy będący stroną trzecią także mogą dostarczać listy konsumentów, których interesuje ogrodnictwo (w oparciu być może o prenumeratę czasopism) lub którzy prawdopodobnie często podróżują (w oparciu być może o przeprowadzony sondaż). Nieustający rozwój w zakresie wykorzystywania danych dotyczących rzeczywistego czasu geograficznego w odniesieniu do profili konsumentów dostarczy kolejnych danych, które pomogą korporacjom skierować kampanie marketingowe do konkretnych konsumentów.

10.2.12. Geograficzne odniesienia nadzoru stwarzają poważne zagrożenie. Usługi i reklama mogą być kierowane jedynie do tych, których uznaje się za bardziej zyskownych. Oceny sytuacji handlowej, oparte na nieustannych odwołaniach do rejestrów kredytowych i tym podobnych, mogłyby doprowadzić do regularnego wykluczania i namierzania osób uznawanych w sektorze handlowym za drugoplanowe w coraz bardziej skomercjalizowanych i unowocześnianych centrach miejskich.

10.2.13. Jeśli chodzi o policję, zaklasyfikowanie przestępcy do kategorii „recydywista” lub „notoryczny recydywista” jest procedurą statystyczną, podczas której punktem odniesienia jest liczba skazań w określonym okresie, przy czym jednostkom są przydzielane numery rejestracyjne wpisywane do głównego komputera policji. Ta klasyfikacja umożliwia intensywne namierzanie danej osoby i podejmowanie interwencji przez różne sądy w ramach strategii skierowanej przeciwko recydywistom.¹⁰⁸ Po zaklasyfikowaniu takiej osoby zostanie ona wprowadzana do systemu J-track przeznaczonego do śledzenia recydywistów i postępowania z nimi na wszystkich etapach działania systemu sądownictwa.

10.3. *Niezamierzona kontrola*

¹⁰⁷ Także w tym przypadku istnieją ograniczenia prywatności w ramach wykorzystywania informacji i ich wymiany między firmami, a mimo to pewne klauzule dopuszczają taki scenariusz, zwłaszcza jeśli materiał marketingowy pochodzi bezpośrednio od pierwotnego właściciela danych, czyli w tym przypadku banku.

¹⁰⁸ Ministerstwo Spraw Wewnętrznych [Home Office] (2004) *Prolific and Other Priority Offender Strategy Initial Guidance* [Wstępne wytyczne dotyczące strategii postępowania z recydywistami], http://www.crimereduction.gov.uk/ppo_e.doc

10.3.1. Tym niemniej, mimo że selekcja społeczna jest zarówno zamiarem jak i skutkiem wielu form nadzoru, sam nadzór nie powinien być traktowany na równi z bezpośrednią kontrolą społeczną.¹⁰⁹ Podczas gdy kontrola społeczna, czyli regulacja postępowania jednostek według surowych zasad w celu wprowadzenia ładu społecznego, może być zamiarem nadzoru (i była nim w przeszłości), w większości współczesnych przypadków na zachodzie kontrolne skutki nadzoru są pośrednie i niezamierzone.

10.3.2. Zamiarem nadzoru jest często po prostu skuteczne i sprawne zarządzanie przepływem dóbr, ludzi i informacji.¹¹⁰ Może dotyczyć ludzi, tak jak na przykład londyński system Intelligent Pedestrian Surveillance (Inteligentnego Nadzoru Piesznych – IPS) w metrze¹¹¹ ma na celu rozpoznawanie miejsc, w których przepływ ludzi został zablokowany, a system kart elektronicznych „Oyster”, używanych przez 5 milionów londyńczyków i umożliwiających dostęp do londyńskiego systemu transportu publicznego ma na celu przyspieszenie przemieszania się ludzi przez miasto. Może dotyczyć ludzi pośrednio, tak jak na przykład opłata z tytułu przeciążenia ruchem, która ma na celu zmniejszenie liczby samochodów na londyńskich ulicach, wykorzystując system ANPR rozpoznający tablice rejestracyjne samochodów, których właściciele nie płacą. Innym przykładem jest wykorzystanie w marketingu „Customer Relationship Management” (CRM) (zarządzanie relacjami z klientem)¹¹², który aktywnie poszukuje dostępu do informacji osobowych aktualnych i potencjalnych klientów, aby nawiązać trwałe relacje poza transakcjami handlowymi.¹¹³ Może w całości dotyczyć dóbr, tak jak w przypadku wykorzystania chipów radiowych RFID w kontenerach przewozowych i towarach handlowych.

10.3.3. Tym niemniej, co jednemu wydaje się „skutecznością”, innemu przychodzi na myśl „kontrolę społeczną”; dzieje się tak zwłaszcza w sytuacji, gdy wykorzystywane są silnie spersonalizowane systemy takie jak przeszukiwanie akt zawierających dane na temat tożsamości, które wymagają, aby poszczególni obywatele nieustannie nosili przy sobie niepowtarzalne identyfikatory.¹¹⁴

10.4. Wymiana informacji

10.4.1. Aby umożliwić selekcję społeczną, informacje muszą być dokładne i łatwo dostępne. W wielu krajach, w tym także w Wielkiej Brytanii, istnieje tendencja w kierunku tworzenia bardziej zintegrowanych, „ściśle współpracujących ze sobą” służb publicznych, często poprzez partnerstwo i pracę zespołową kilku organów. Coraz częściej liczne lokalne porozumienia partnerskie łączą ze sobą różne organy i branże, tak aby mogły one wykorzystać swoje kompetencje do większego koncentrowania się na świadczeniu usług

¹⁰⁹ Lianos, M. (2001) *Le Nouveau Contrôle Social toile institutionnelle, normativité et lien social*. Paris: L'Harmattan-Logiques Sociales.

¹¹⁰ Graham, S. i Wood, D. (2003) „Digitising surveillance: categorisation, space and inequality [Dyskredytujący nadzór: klasyfikacja, przestrzeń i nierówność]”, *Critical Social Policy*, 23: 227-248.

¹¹¹ Hogan, J. (2003) „Smart software linked to CCTV can spot dubious behaviour [Inteligentne oprogramowanie połączone z CCTV może rozpoznać podejrzane zachowanie]”, *New Scientist*, 11 July, <http://www.newscientist.com/article.ns?id=dn3918>.

¹¹² CRM obejmuje elektroniczne rozproszenie danych osobowych w celu analizowania i tworzenia długoterminowych relacji z klientami.

¹¹³ Morgan, R.M., and Hunt, S.D (1994) “The commitment-trust theory of relationship marketing [Teoria oparta na zaangażowaniu i zaufaniu w marketingu relacyjnym]”, *Journal of Marketing* 58: 20-38.

¹¹⁴ Aby zapoznać się z krytyczną opinią naukowca specjalizującego się w komputerach, zob.: Clarke, R. (2006) „National identity cards? Bust the myth of 'security über alles'! [Krajowe dowody tożsamości? Obalić mit 'bezpieczeństwa über alles!']”, <http://www.anu.edu.au/people/Roger.Clarke/DV/NatID-BC-0602.html>

jednostkom w bardziej zintegrowany sposób.¹¹⁵ Głównym punktem programu modernizacji New Labour było przekształcenie grupy różnych organów w skoordynowany i współpracujący ze sobą system przy dużej inwestycji w IT.

10.4.2. Jednym z efektów tej kluczowej realizacji jest fakt, że granice, o których myślano dawniej, że zapewniały pewną, choć słabą, ochronę prywatności i ograniczenia nadzoru, zostały podane w wątpliwość, często wprawiając podmioty świadczące usługi publiczne w osłupienie z powodu rozbieżności pomiędzy obecnym system zarządzania informacjami osobowymi, a tym który powinien być stosowany. Wprowadzono przepływ danych osobowych nowymi kanałami, także prywatnymi, przez organizacje, które nigdy przedtem nie miały do nich dostępu i których tradycje dotyczące poufności i ochrony prywatności mogą znacznie różnić się między sobą, jak również odbiegać od tradycji podmiotów sektora publicznego.

10.4.3. Walka z przestępczością gospodarczą jest istotnym przykładem. Ustawa o administracji zabezpieczenia społecznego (oszustwa) z 1997 r. dała możliwość podejmowania wielu działań, w tym wymieniać się informacjami i zestawiać ich ze sobą, a następnie w 2001 r. weszła kolejna ustawa zezwalająca na dostęp do rachunków bankowych i oszczędnościowych osób prywatnych i do rachunków przedsiębiorstwa oraz rejestrów zakładu użyteczności w publicznej, a w niektórych przypadkach także do list płac sektora prywatnego. W ramach ustawy z 1997 r. Ministerstwo Pracy i Emerytur (Department for Work and Pensions, DWP) dokonuje wielu rutynowych zestawień danych umożliwiających identyfikację osób, korzystając także z rejestrów zawierających informacje na temat dodatków mieszkaniowych, opieki społecznej, systemu ubezpieczeń społecznych, jak również gazu, elektryczności i telefonów. DWP aktywnie sprawdza tożsamość petentów i związki z innymi organami publicznymi. Co więcej, Komisja Audytu realizuje co roku zakrojone na szeroką skalę działania polegające na zestawianiu danych w ramach National Fraud Initiative (Krajowej Inicjatywy w związku z Przestępczością Gospodarczą – NFI). Celem jest udzielanie pomocy w wykrywaniu nielegalnych i zbyt dużych wypłat z funduszy publicznych dla petentów.¹¹⁶ Oszustwa związane z dodatkami mieszkaniowymi nadal stanowią główny problem, ale NFI ma obecnie szerokie pole działania dzięki informacjom, do których ma dostęp. Wykorzystuje dane pochodzące z listy wypłat lokalnych organów ds. zdrowia i rejestry zawierające informacje o emeryturach, jak również rejestry zawierające informacje na temat dzierżawców, dodatków mieszkaniowych, akt opieki społecznej i osób ubiegających się o azyl. Szacunki wartości pieniężnej nielegalnych płatności bardzo się od siebie różnią, ale przypuszczalnie opiewają na kilka miliardów funtów, podczas gdy rezultaty działań zmierzających do ich wyeliminowania zostały ocenione o wiele niżej, na około 126 funtów w okresie 2004-2005, wliczając Szkocję.¹¹⁷ To niewielki ułamek tego, co wypłacono w dodatkach i obejmuje nadpłaty, które nie są nielegalne. Mimo że oszustwo pozostaje oszustwem, powstają pytania o proporcjonalność, przejrzystość i inne skutki dla prywatności związane z metodami „zapchania dziury” w wydatkach publicznych, wymagającymi wielu danych.

¹¹⁵ 6 et al. 2005 op cit. n.24; Bellamy et al., 2005 op cit. n.24.

¹¹⁶ Komisja Audytu [Audit Commission] (nd.) *National Fraud Initiative (NFI)* [Krajowa inicjatywa walki z przestępczością gospodarczą], <http://www.audit-commission.gov.uk/nfi/>.

¹¹⁷ Komisja Audytu [Audit Commission] (nd.) *National Fraud Initiative 2004-5* [Krajowa inicjatywa walki z przestępczością gospodarczą 2004-2005], http://www.audit-commission.gov.uk/nfi/downloads/NFI_2004-05Summary.pdf.

10.4.4. Najnowszy dokument konsultacyjny Ministerstwa Spraw Wewnętrznych¹¹⁸ zawiera rozważania na temat zdobywania nowych sposobów walki z zorganizowaną przestępczością finansową, podkreślając, że „wymiana danych z innymi stronami sektora publicznego odbywa się bardzo nieregularnie, a wymiana pomiędzy sektorem publicznym a prywatnym ma miejsce bardzo rzadko”.¹¹⁹ Dokument ten opowiada się za usprawnieniem przepływu informacji, w tym – w odniesieniu do raportów o podejrzanym działaniu – zestawianie danych nowej agencji do walki z przestępczością zorganizowaną (Serious Organized Crime Agency, SOCA) z bazami danych licznych organów rządowych, w tym Królewskiego Urzędu Podatkowego i Celnego (Her Majesty's Revenue and Customs), wydziału komunikacji (Driver and Vehicle Licensing Agency), DWP oraz urzędu paszportowego. Obecnie podejmowane są nowe inicjatywy, wliczając w to nowy komitet ministerialny ds. wymiany danych (Ministerial Committee on Data-Sharing, MISC 31)¹²⁰, kompetentny w zakresie „opracowania strategii rządowej dotyczącej wymiany danych w sektorze publicznym”.

10.4.5. Jak już mogliśmy się przekonać, policja dysponuje nowymi bazami danych, w których gromadzone są szczegółowe informacje na temat obywateli i przestępców, aby zagwarantować, że informacje są wymieniane pomiędzy wszystkimi organami biorącymi udział w programie rządowym mającym na celu zmniejszenie przestępczości. Efektem znacznych inwestycji w systemy IT i oprogramowanie w całym sądownictwie karnym było umożliwienie zintegrowania różnych baz danych i odwoływania się do nich w całej policji i we wszystkich organach sądownictwa karnego. W konsekwencji obecnie dostępny jest jeden plik główny. I tak na przykład przejeżdżające pojazdy są rejestrowane przez system ANPR, ich numery rejestracyjne są zapamiętywane, a następnie sprawdzane w rejestrze DVLC zarejestrowanych pojazdów i ich zarejestrowanych właścicieli. Taka informacja pozwala uzyskać dostęp do innych baz danych dostępnych w ramach PNC, takich jak baza danych odcisków palców, przeszłości kryminalnej lub rejestru osób, które dokonały przestępstw na tle seksualnym lub z wykorzystaniem przemocy, a także do baz danych ubezpieczycieli oraz baz danych MOT. Zakres integracji został zilustrowany w systemie ANPR policji Hertfordshire, która ma dostęp do 40 krajowych i lokalnych baz danych podczas śledzenia pojazdu¹²¹.

10.4.6. Tym niemniej wymiana informacji sięga o wiele dalej. Wraz z rozpoczęciem łączenia organów w celu zmniejszenia zagrożenia przestępczością i ponownymi wykroczeniami znacznie zatęchły granice pomiędzy informacjami na temat sądownictwa karnego a informacjami przechowywanymi przez innych. Na przykład zespoły ds. przestępczości nieletnich składają się z przedstawicieli policji, systemu nadzoru kuratorskiego, opieki społecznej, służb ds. zdrowia, edukacji i nadużywania narkotyków oraz alkoholu, a także lokalnych urzędników i jeśli oni wszyscy podpisali protokół w sprawie wymiany informacji, mogą przekazywać sobie informacje na temat osób prawnych i rodzin w ramach własnej jurysdykcji.¹²² Podobnie system

¹¹⁸ Ministerstwo Spraw Wewnętrznych [Home Office] (2006) *New Powers Against Organised and Financial Crime* [Nowe siły przeciwko zorganizowanej przestępczości finansowej] (Cm 6875). London: The Stationery Office.

¹¹⁹ *ibid.*: 12

¹²⁰

<http://www.cabinetoffice.gov.uk/secretariats/committees/misc31.asp>.

¹²¹ Hertfordshire Constabulary [Policja Hertfordshire] (2005) “The human chassis number [Podstawowe numery dla ludności]”, wniosek o udział w Tilley Award, <http://www.popcenter.org/Library/Tilley/2005/05-02.pdf>.

¹²² Aby zapoznać się z dyskusją na temat zespołów do spraw nieletnich (Youth Justice Teams), zob.: Newburn, T. (2004) *Crime and Criminal Justice Policy* [Polityka sądownictwa karnego], Harlow: Longman, 211ff.

identyfikacji, kierowania i śledzenia (Identification, Referral and Tracking System), opracowany w odpowiedzi na dochodzenie w sprawie Climbié, stworzył „węzeł informacyjny” umożliwiający lekarzom dostęp do wszystkich informacji przechowywanych przez liczne służby ds. dzieci, w tym policję i zespoły ds. przestępczości nieletnich.¹²³

10.4.7. System ten działa także poza granicami kraju. Na przykład nowe systemy identyfikacji tożsamości podlegają globalizacji, ponieważ rządy starają się „zharmonizować” procedury identyfikacji, co ułatwiają nowe technologie. Międzynarodowa Organizacja Lotnictwa Cywilnego (International Civil Aviation Organization) odgrywa w tym wiodącą rolę, wyznaczając standardy dla paszportów biometrycznych i bezpośrednio dla programów elektronicznych dowodów tożsamości. Organizowane są międzynarodowe konwencje, aby opracować „interoperacyjne systemy globalne” do identyfikacji dokumentów podróży odczytywanych automatycznie (Machine-Readable Travel Documents, MRTD).¹²⁴ Chociaż nie oznacza to, że trzeba wymieniać się informacjami, zapewnia infrastrukturę potrzebną do umożliwienia tej wymiany.

10.4.8. Kontakty między różnymi korporacjami telekomunikacyjnymi są potencjalnie globalne. W przypadku świadczenia zarówno usług telefonii komórkowej jak i usług internetowych, operatorzy sieci i operatorzy świadczący usługi internetowe działają także poza granicami kraju, przy czym dane między nimi są przekazywane przez organizacje zależne lub kontraktowe. Jednak wyzwanie, przed którym stoją organy regulacyjne, staje się nawet jeszcze bardziej złożone.

10.4.9. W sektorze prywatnym przejawia się przybierająca na sile ogólna tendencja, aby integrować obszerne zbiory danych mające największe znaczenie w nadzorze konsumenckim, przy czym wiele przedsiębiorstw aktywnie stara się rozszerzyć swoje aktualne bazy danych. Niektóre firmy opracowały strategię oparte na wspólnym korzystaniu z baz danych wraz z innymi przedsiębiorstwami. Partnerzy programów koalicyjnych, takich jak te tworzone w sektorze marketingu lojalnościowego, często zawierają porozumienia w sprawie wymiany danych, zwykle przez głównego partnera koalicji, jednak istnieje także tendencja w kierunku tworzenia spółdzielni danych, których członkowie wymieniają się między sobą zgromadzonymi danymi. Ponad 50% ludności Zjednoczonego Królestwa posiada jedną z kart lojalnościowych Nectar obsługiwanych przez system zarządzania programami lojalnościowymi (Loyalty Management UK). 216 skatalogowanych przedsiębiorstw w Zjednoczonym Królestwie przystąpiło do konsorcjum wymiany danych Abacus, dysponującego informacjami na temat 26 milionów konsumentów indywidualnych, rozszerzanymi przez Claritas' Lifestyle Universe. Obejmują one dane na temat dochodów, stylu i etapu życia każdego z tych konsumentów.¹²⁵

10.5. *Zacieranie granic pomiędzy sektorem publicznym a sektorem prywatnym*

¹²³ Aby zapoznać się z dyskusją na temat sprawy Climbié, zob.: Parton, N. (2006) *Safeguarding Childhood: Early Intervention and Surveillance in Late Modern Society* [Ochronić dzieciństwo: wczesna interwencja i nadzór we współczesnym społeczeństwie], Basingstoke: Palgrave Macmillan, Ch3.

¹²⁴ Zob.: ICAO (2003) *MRTD: Machine Readable Travel Documents* [Dokumenty podróży odczytywalne komputerowo], <http://www.icao.int/mrtd/Home/Index.cfm>.

¹²⁵ Evans, M. (2005) „The data-informed marketing model and its social responsibility [Model marketingowy gromadzący dane i jego odpowiedzialność społeczna]”, w: Lace, S (2005) *op cit.*, n.6.

10.5.1. Tym niemniej, mimo że sektor publiczny wymienia się informacjami z sektorem prywatnym i odwrotnie, coraz bardziej zacierają się granice pomiędzy interesami tych sektorów, w miarę jak coraz więcej zadań rządowych jest realizowanych za pomocą często złożonych mechanizmów łączących sektory: publiczny, prywatny i społeczny, a czasem wykorzystujących tylko jeden z nich. Coraz częściej lokalne porozumienia partnerskie łączą ze sobą różne organy i branże, tak aby móc wykorzystać swoje kompetencje do większego koncentrowania się na świadczeniu usług jednostkom w bardziej zintegrowany sposób.¹²⁶ W sytuacji, gdy informacje będące w posiadaniu państwa są dostępne do użytku prywatnego, tak jak to sugerowano przy okazji narodowego rejestru tożsamości (National Identity Register, NIR), należy zastanowić się, jakie są ograniczenia dostępu dla ludzi jako obywateli i jako konsumentów i gdzie przebiegają granice.

10.5.2. Bezpośrednia prywatyzacja może czasem być kluczem do wzmożonego nadzoru. Telekomunikacja odgrywa tutaj istotną rolę; wraz z dywersyfikacją i konwergencją technologii i funkcji w telekomunikacji, dywersyfikacja rynków telekomunikacyjnych znacznie rozszerzyła nadzór. Na początku lat 80-tych utworzono British Telecommunications (BT) jako samodzielną jednostkę, którą prawie natychmiast sprywatyzowano, a także otwarto rynek na konkurencję w sektorze telekomunikacji i powołano urząd ds. telekomunikacji (Office of Telecommunications) w charakterze organu regulacyjnego sektora. Podział obowiązków organizacyjnych doprowadził w konsekwencji do tego, że liczba organizacji potencjalnie zachowujących i eksplorujących dane telekomunikacyjne wzrosła wykładniczo.

10.5.3. Prywatyzowano nawet praktyki nadzoru granicznego. Rezultat jest taki, że straż graniczna coraz częściej korzysta z usług prywatnych przedsiębiorstw handlowych - międzynarodowych przedsiębiorstw IT, głównych producentów broni i sprzętu wojskowego, konsultantów, analityków ryzyka, banków oraz korporacji zajmujących się zarządzaniem tożsamością i biometrią. Na przykład w 2004 r. IBM wygrał kontrakt na 15 milionów funtów w ramach „Project Semaphore”, pierwszego etapu programu rządowego Zjednoczonego Królestwa o nazwie e-Borders. Project Semaphore, w programie podobnym do USVISIT, integruje bazy danych na temat pasażerów linii lotniczych, którzy wkracają na teren Zjednoczonego Królestwa lub go opuszczają. Wraz z „Project Iris”, także testowanym przez IBM, program doda dane biometryczne do zintegrowanych baz danych, które mogą rozpoznać nietypowe zachowania. IBM jest jednym z szerokiego wachlarza przedsiębiorstw, które realizują obecnie „praktykę bezpieczeństwa krajowego”, oferując rządowi zarządzanie danymi, metody biometryczne i usługi w zakresie identyfikacji tożsamości. Innymi godnymi uwagi firmami są: Accenture, która stoi na czele US Smart Borders Alliance o wartości 10 miliardów dolarów w Stanach Zjednoczonych; Oracle, którego wszechobecne systemy zarządzania tożsamością są stosowane w Zjednoczonym Królestwie i Stanach Zjednoczonych jako „rozwiązania w ramach bezpieczeństwa krajowego”; przedsiębiorstwa zajmujące się elektronicznymi i telekomunikacyjnymi produktami konsumenckimi, takie jak Ericsson, które są wykonawcami w ramach amerykańskiej strategicznej inicjatywy granicznej (Strategic Border Initiative, SBI).

10.5.4. W wielu przypadkach graniczne systemy biometryczne są połączone z programami przeznaczonymi dla osób, które często podróżują liniami

¹²⁶ 6 et al. 2005 op cit. n.24; Bellamy et al., 2005 op cit. n.24.

lotniczymi oraz innymi programami kart lojalnościowych, a w Stanach Zjednoczonych istnieje tendencja wspólnego sponsorowania przez kredytodawców, takich jak Mastercard. Rozwój sprywatyzowanej „gwarancji identyfikacji tożsamości” może sprawić, że niektóre bazy danych krajowych dowodów tożsamości i paszportów biometrycznych staną się przestarzałe.

10.5.5. Istnieje także wyraźny ruch w kierunku włączenia grup obywatelskich i grup obserwacyjnych do realizacji praktyk bezpieczeństwa krajowego. Jest on najbardziej zaawansowany w Stanach Zjednoczonych, gdzie w ramach programów, takich jak Highway Watch, Citizen Corps, Coast Watch i River Watch, szkoli się obywateli, tak aby potrafili „rozpoznawać nietypowe działania”. Jeden z elementów tej formy praktyk codziennego nadzoru w sposób szczególny odbił się echem w dziedzinie nadzoru granicznego. Dla wielu prywatnych przedsiębiorstw, które stają do przetargów na kontrakty w ramach nadzoru granicznego bądź je wygrywają, elektroniczne produkty konsumenckie, takie jak telefony komórkowe, notesy elektroniczne i palmtopy, mają istotne znaczenie. Na przykład firma IBM podpisała kontrakt na system e-Borders w Zjednoczonym Królestwie, a także zasponsorowała program obywatelskiego bezpieczeństwa krajowego w Stanach Zjednoczonych, który pozwolił połączyć cyfrowo program bezpieczeństwa sąsiedzkiego z programem bezpieczeństwa krajowego za pomocą laptopów, telefonów komórkowych i urządzeń elektronicznych.

10.5.6. Ostatecznie państwo może podjąć próby, aby zdominować albo osłabić międzynarodowe lub prywatne organizacje, które dostarczają produkty informacyjne lub które regulują infrastrukturę informacyjną. Amerykańska Agencja Bezpieczeństwa Narodowego (NSA) nawiązała stosunki robocze z większością najważniejszych amerykańskich przedsiębiorstw działających na rynku oprogramowania i sprzętu komputerowego, dzięki czemu kodowanie systemów przede wszystkim w eksportowych wersjach oprogramowania jest mniej skomplikowane niż w wersjach dostępnych na rynku krajowym w Stanach Zjednoczonych i łatwiej je skrakować. NSA i Centrala Łączności Rządowej (GCHQ) także zawiera porozumienia z przedsiębiorstwami międzynarodowej sieci kablowej (International Licensed Cable, ILC), aby umożliwić przejście. Zwłaszcza NSA poinformowała, że ma przedstawicieli w komitetach wyznaczających standardy transgraniczne, przede wszystkim MFA Forum (wcześniej Frame Relay Forum) – niezależnym organie odpowiedzialnym za opracowanie powszechnych standardów przekazywania danych, w skład którego wchodzi także wszystkie najważniejsze przedsiębiorstwa telekomunikacyjne i komputerowe z państw uprzemysłowionych¹²⁷.

10.5.7. Istnieją zatem liczni przedstawiciele i organy ds. nadzoru, dysponujący często własnymi bazami danych, którzy coraz częściej spotykają się z naciskami ze strony sektora handlowego, aby kupować i sprzedawać cenne informacje, a także ze strony państwa, które życzy sobie, aby gromadzić informacje do celów walki z terroryzmem i przestępczością gospodarczą oraz egzekwowania prawa.

11. Społeczne konsekwencje nadzoru

¹²⁷ Seeberg, K. i Elkjær, B. (1999) ”Tele Danmark in a club with Echelon spies [Tele Dania w klubie ze szpiegami systemu Echelon]”, *Ekstra Bladet* (Denmark), 26 września. Forum MFA można znaleźć na <http://www.mfaforum.org/>.

11.1. Zajmiemy się teraz konsekwencjami społecznymi nadzoru technologii i procesów, które przedstawiliśmy w poprzednich działach. Krytyka nadzoru najczęściej dotyczy prywatności, dlatego też jest to bez wątpienia podstawowa kwestia, mimo że sami wolelibyśmy omówić ją jako jeden z aspektów indywidualnej autonomii. Tym niemniej chcielibyśmy także zwrócić uwagę na o wiele rzadziej poruszane kwestie związane z rezultatami decyzji i zgody i co najważniejsze, na wpływ procesów selekcjonowania, klasyfikowania i namierzania na szanse życiowe jednostek i całych grup lub wspólnot, ich relatywną mobilność oraz dostęp do możliwości.

11.2. *Autonomia: anonimowość i prywatność*

11.2.1. Na autonomię jednostek składa się wiele elementów; omówimy tutaj dwa spośród nich, na które szczególnie oddziałuje nadzór. Pierwszym z nich jest anonimowość. Anonimowość od dawna była postrzegana jako jeden z kluczowych aspektów współczesnego życia, zwłaszcza w mieście. Nadzór może z pewnością pomóc stworzyć wiele nowych usług, przyspieszony tryb życia w mieście charakteryzujący się usługami dopasowanymi do jednostek oraz nieustającą interakcją elektroniczną i fizyczną, zawsze działającą gospodarkę cyfrową i przejrzystość wielu barier czasowych oraz przestrzennych, które tradycyjnie krępowały życie miejskie. Tym niemniej jedną z pierwszych ofiar wszechobecnego nadzoru, zwłaszcza systemów identyfikacji tożsamości, jest właśnie anonimowość, która pozwala ludziom uciekać przed strukturami intensywnego nadzoru małych wspólnot. Ogólny wstępny warunek anonimowości na wiele sposobów umożliwia jednostce tworzenie własnej tożsamości poprzez swoje działania i relacje.

11.2.2. Spośród półtora miliona osób skazanych przez sądy w 2003 r., około 107 000 skazano na natychmiastowy areszt.¹²⁸ Wyrok skazujący na uwięzienie nie tylko oznacza utratę wolności, ale wiąże się także z utratą innego ważnego elementu autonomii, prywatności. W więzieniach Zjednoczonego Królestwa wszyscy przestępcy znajdują się pod stałym nadzorem. Od 1996 r. system nadzoru obejmował obowiązkowe testy na obecność narkotyków przy założeniu, że co miesiąc zostanie poddanych testom od 5 do 10 procent więźniów.¹²⁹ W okresie 2004-2005 wykonano 51 484 testy, z czego 11,6 % dało pozytywne wyniki.¹³⁰ Także przestępcy wypuszczani z więzienia są często przedmiotem monitorowania elektronicznego, stosowanego albo w przypadku wcześniejszego zwolnienia z zakładu karnego w ramach brytyjskiego programu „Home Detention Curfew Scheme”¹³¹, albo w przypadku zwolnienia warunkowego.¹³²

11.2.3. Inną stosunkowo często ograniczaną grupę stanowią pacjenci. Autonomia, godność i prawo do prywatności pacjenta zawsze rodziły poważne wątpliwości. Dane dotyczące zdrowia często uważane są za dane podlegające szczególnej ochronie, mimo że stopień ochrony, jakiej podlegają, może być różny. Wielu przedstawicieli sektora martwi się, czy można zachować

¹²⁸ Home Office [Ministerstwo Spraw Wewnętrznych] (2005) *Sentencing Statistics 2003: England and Wales* [Statystyki dot. wyroków 2003; Anglia i Walia], London: Home Office, 3.

¹²⁹ Singleton, N. et al. (2005) *The Impact and Effectiveness of Mandatory Drug Testing in Prisons* [Wpływ i skuteczność obowiązkowych testów na obecność narkotyków w więzieniu], Home Office Research Findings 223, London Home Office.

¹³⁰ HMPS (Her Majesty's Prison Service – Królewska Służba Więzienna) (2005) *Her Majesty's Prison Service Annual Report and Accounts* [Roczny raport i relacje Królewskiej Służby Więziennej], załącznik 1: Statistical Information, London: Stationery Office, 110.

¹³¹ System HDC umożliwia zwolnienie osób skazanych na pobyt w więzieniu od 3 miesięcy do mniej niż 4 lata od 2 tygodni do czterech i pół miesiąca wcześniej, pod warunkiem że prowadzony będzie elektroniczny monitoring tychże osób. W okresie 2004-2005 w ramach tego systemu zwolniono wcześniej 19096 osób. Zob.: NPS (2006) *op cit.* n.82.

¹³² *ibid.*

tradycyjne założenia dotyczące poufności, kiedy w grę wchodzi na przykład „jednoosobowe oceny” tych pacjentów, którymi zajmuje się opieka społeczna lub również lekarze, albo w sytuacji, gdy może istnieć konieczność przekazania danych na temat zdrowia psychicznego pacjentów innym organom, czasem także policji. Przez prawie dziesięć lat funkcjonował system „Caldicott Guardians”, nazwany tak na cześć autora raportu dotyczącego poufności możliwych do zidentyfikowania danych o pacjentach w państwowej służbie zdrowia (NHS)¹³³. To oznacza, że w ramach każdego organu NHS jest osoba odpowiedzialna za nadzorowanie poufności, kontrolowanie informacji o pacjentach, pomaganie w sporządzaniu protokołów w ramach wymiany informacji pomiędzy organizacjami i zapewnianie dobrej praktyki w odniesieniu do danych dotyczących pacjentów. System ten jest częścią większej struktury „zarządzania informacjami” w NHS, a obecnie wykorzystuje się go także w agencjach opieki społecznej. Jednak bez względu na to jak funkcjonował system „strażniczy” – rezultaty różniły się od siebie i pojawiło się wiele nieprawidłowości spowodowanych takimi czynnikami jak złożoność technologii informacyjnych „eHealth” i przepływu informacji, niewystarczające zasoby i niewystarczające szkolenie oraz słabe wsparcie roli instytucjonalnej¹³⁴ – wokół ujawniania danych dotyczących zdrowia rodziło się wiele kontrowersji w kontekście antyterroryzmu, walki z przestępczością i dochodzeń Komisji Audytu. Ministerstwo Zdrowia opracowało strategię poufności i kodeks postępowania w związku z prywatnością i poufnością¹³⁵, a Rzecznik ds. Informacji przygotował wytyczne dla sektora zdrowia, kiedy rosły obawy odnośnie do wymiany danych NHS z innymi agencjami.¹³⁶

11.2.4. Kwestie prywatności dotyczą często także nadzoru w miejscu pracy. Przy omawianiu zagadnień związanych z prywatnością w tej dziedzinie ważne jest, aby skupić się na całej gamie koncepcji dotyczących prywatności: prywatność a ludzkie ciało, prywatność w relacjach społecznych, prywatność a przestrzeń osobista, jak również prywatność informacji¹³⁷. Ważne jest także, aby rozważyć wszystkie możliwe konsekwencje ujawnienia: czy pracownicy wyrazili zgodę na przekazywanie danych na temat swojego ciała, relacji społecznych, przestrzeni osobistej i informacji i czy wiedzieli, kto będzie stroną w wymianie tych danych.¹³⁸

11.2.5. Osoby ubiegające się o pracę może zniechęcić zwłaszcza procedura testowania na obecność narkotyków. Testy nie odróżniają osób uzależnionych od tych, które raz na jakiś czas sięgają po narkotyki, a kilkudniowa abstynencja

¹³³ Department of Health (Ministerstwo Zdrowia) (1997) *Report on the Review of Patient Identifiable Information [Raport w sprawie przeglądania możliwych do rozpoznania informacji o pacjentach]* (The Caldicott Report). London: Department of Health.

¹³⁴ NHS Scotland (2004) *A Review of the Work of the Caldicott Guardians [Przegląd pracy strażników Caldicott]*, <http://www.confidentiality.scot.nhs.uk/publications/Caldicott%20Review.pdf>

¹³⁵ Department of Health (Ministerstwo Zdrowia) (2001) *Building the Information Core: Protecting and Using Confidential Patient Information [Tworzenie trzonu informacyjnego: ochrona i wykorzystywanie poufnych informacji o pacjentach]*, London: Department of Health; Department of Health (Ministerstwo Zdrowia) (2003) *Confidentiality: NHS Code of Practice [Poufność: Kodeks postępowania NHS]*, London: Department of Health.

¹³⁶ Office of the Information Commissioner [Biuro Rzecznika ds. Informacji] (2002) *Use and Disclosure of Health Data: Guidance on the Application of the Data Protection Act 1998 [Wykorzystanie i ujawnianie danych dotyczących zdrowia: wytyczne dotyczące stosowania ustawy o ochronie danych z 1998 r.]*, Wilmslow: Office of the Information Commissioner.

¹³⁷ Laurent, C. i organizacja Privacy International (2003) *Privacy and Human Rights 2003. An International Survey of Privacy Laws and Developments [Prywatność i prawa człowieka 2003. Międzynarodowy sondaż na temat ustaw i opracowań na temat prywatności]*, Washington DC / London: Electronic Privacy Information Centre (EPIC) / Privacy International. <http://www.privacyinternational.org/survey/phr2003/>.

¹³⁸ Ball, K. (2001) “Situating workplace surveillance: ethics and computer based performance monitoring” [Lokalizowanie nadzoru w miejscu pracy: etyka a monitoring komputerowy], *Ethics and Information Technology [Etyka a technologia informacji]*, 3(3): 211-223.

przed testem przeważnie gwarantuje wynik negatywny.¹³⁹ Uprawnienia pracodawców do nagrywania i przechowywania informacji przekazywanych przez pracowników także wywołuje obawy, dlatego że po pierwsze prywatne rozmowy mogą zawierać poufne informacje (np. numer karty kredytowej), po drugie informacje te mogą być przechowywane na serwerach zagranicznych podlegających innym jurysdykcjom, a po trzecie z powodu szerokiego zakresu i zasięgu tych strategii. Trudno określić odpowiednią strategię w odniesieniu do tajnego nadzoru. Toczy się debata na temat, czy firmy powinny powiadamiać personel, że może być potajemnie nadzorowany lub czy można tego całkiem uniknąć. Gromadzenie informacji osobowych na temat pracowników i innych informacji o ich życiu może zagrażać prywatności, jeśli pracownicy nie wyrażają zgody na ujawnianie dotyczących ich informacji i przekazywanie ich stronom trzecim.¹⁴⁰

11.2.6. W tym kontekście musimy powrócić do proponowanego krajowego systemu identyfikacji tożsamości. Ostatni raport¹⁴¹ Komisji Izby Gmin (House of Commons Select Committee) zawierał skargi na rażąco niejasny zakres proponowanych funkcji dowodów tożsamości. Ta najbardziej kontrowersyjna w Wielkiej Brytanii kwestia obejmuje potencjalne zagrożenia prywatności z powodu wprowadzenia i wykorzystywania NIR utworzonego w ramach ustawy o dowodach tożsamości z 2006 r. Dowody tożsamości będą nie tylko umożliwiały Ministerstwu Spraw Zagranicznych pełnienie tradycyjnych funkcji w odniesieniu do egzekwowania prawa (mówiąc ogólnie), imigracji i azylu, bezpieczeństwa narodowego i antyterroryzmu, ale ich zadaniem będzie także „zapewnienie skutecznego i efektywnego świadczenia usług publicznych” w sposób ukierunkowany, choć włączający potencjalnie wiele ministerstw i organów związanych z konkretnymi obszarami usług. Kluczowym elementem jest przyporządkowanie każdej osobie niepowtarzalnego numeru referencyjnego, ułatwiającego integrowanie licznych danych źródłowych. Co więcej oznaki, że rząd przewiduje wzajemne relacje pomiędzy sektorami publicznym i prywatnym w zakresie wykorzystywania dowodów tożsamości, wliczając dostęp do NIR, rodzą dodatkowe obawy o ograniczenia i ochronę prywatności przy możliwym rozszerzeniu nadzoru.

11.2.7. Mimo że ustawy o ochronie danych i prywatności¹⁴² zostały opracowane w celu ograniczenia takich działań, okazało się, że bardzo ciężko jest dotrzymać kroku zmianom technicznym lub pomysłowości osób, które próbują uniknąć regulacji. Jeśli system dowodów tożsamości Zjednoczonego Królestwa ma, zgodnie z zapowiedziami, chronić przed „kradzieżą tożsamości”, można przypuszczać, że dostępne będą dane handlowe dotyczące banków i kart kredytowych, jak również dane dotyczące organów administracji rządowej na przykład w zakresie imigracji albo zdrowia.

11.2.8. Jeśli chodzi o organy regulujące kwestie prywatności, kładzie się coraz większy nacisk na ograniczenie celów wykorzystywania danych osobowych, okresu przechowywania danych i tym podobnych. Wykorzystanie

¹³⁹ Testy na obecność narkotyków wskazują jedynie obecność zażywanych narkotyków. Komentatorzy określają je mianem „testów na inteligencję”: żeby oblać, kandydat musi być bardzo głupi!

¹⁴⁰ Aby uzyskać więcej informacji na temat monitorowania e-maili, zob.: Lloyd, J. (2006) „Management email monitoring brings Big Brother to mind [Monitorowanie e-maili przez kadrę kierowniczą przywołuje na myśl Wielkiego Brata]”, *Receivables Report for Americas Health Care Financial Managers* [Raporty na temat wiarygodności dla dyrektorów finansowych amerykańskiej służby zdrowia] 21(1): 6-7

¹⁴¹ House of Commons Science and Technology Committee [Izba Gmin, Komisja ds. Nauki i Technologii] (2006) *Sixth Report [Szósty raport]*, HC 1032, London: The Stationary Office.

¹⁴² Zob. np.: UK ‘Data Protection Act’ 1998 [Ustawa o ochronie danych z 1998 r.], <http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

elektronicznych, telekomunikacyjnych produktów konsumenckich codziennego użytku do przekazywania danych, informacji lub obrazów z prywatnych domen do sfery władz publicznych zaciera granice pomiędzy sektorami publicznym i prywatnym. Zgodnie z komentarzem ACLU po przeprowadzeniu badań nad nową siecią nadzoru, przedsiębiorstwa i obywatele są nieustannie „werbowani do szeregów powstającego społeczeństwa nadzorowanego”.¹⁴³

11.2.9. Mimo że ludzie często decydują się na nadzór konsumencki dobrowolnie (kupić czy nie kupić?), ma on i tak istotny wpływ na prywatność, co sugeruje, że zakres nadzoru konsumenckiego powinien zostać ograniczony. Ustawodawstwo dotyczące prywatności w Unii Europejskiej i w krajach, które wprowadziły podobne zbiorowe ustawodawstwo przewidujące ograniczenia w zakresie gromadzenia i wykorzystywania danych osobowych, wymaga, aby wyznaczyć cele, jak również zapewnić ochronę bezpieczeństwa danych osobowych. Dwie spośród praktyk ochrony danych zawartych w ustawodawstwie są niekompatybilne z technikami eksploracji danych, które leżą u podstaw nadzoru konsumenckiego. Po pierwsze, wykorzystanie danych nie może zostać jasno przedstawione konsumentowi. Niemożliwe jest przewidzenie wyników analizy danych przeprowadzonej przy wykorzystaniu technologii wyznaczonej do wykrywania nieoczywistych relacji i wzorów w zestawach danych. Oznacza to, że przedsiębiorstwa nie są w stanie w pełni informować klientów o wykorzystywaniu ich danych, ponieważ kategorie utworzone w wyniku analizy danych są nowe. Po drugie, zasada ograniczenia wykorzystania informacji blokuje każdy cel w ramach gromadzenia i wykorzystywania danych konsumenta. Rosnąca liczba danych i potencjalnych zmiennych sprawia, że predykatywność systemu jest coraz dokładniejsza.¹⁴⁴ Prócz tego, mimo że ustawodawstwo o prywatności ogranicza wykorzystanie możliwych do rozpoznania informacji osobowych, informacje uzyskane z tych identyfikatorów mogą nadal być wykorzystywane w ramach praktyk nadzoru konsumenckiego. A to może z kolei mieć takie same skutki dla tych kategorii konsumentów wysokiego ryzyka.

11.2.10. Na szczególną uwagę w telekomunikacji bezprzewodowej zasługuje rozróżnienie pomiędzy przechowywaniem i monitorowaniem informacji dotyczących „przekazywania”, niezbędnych do wymiany informacji (w większości generowanych automatycznie) a przechowywaniem i monitorowaniem informacji „osobowych”, takich jak imię, adres i szczegółowe informacje dotyczące płatności, tym samym podlegających zapisom odpowiedniego ustawodawstwa o ochronie danych. Oczywiście operatorzy sieci telefonów komórkowych i podmioty świadczące usługi w zakresie telefonii komórkowej gromadzą i przechowują szeroki wachlarz danych.

11.2.11. Jeśli chodzi o egzekwowanie prawa przez państwo i nadzór polityczny, podział ma mniejsze znaczenie. Ustawa o uprawnieniach śledczych z 2000 r. zezwala na udostępnianie danych dotyczących ruchu w sieci i naliczania opłat na wniosek organizacji egzekwujących prawo Zjednoczonego Królestwa. W ramach RIPA wyższy rangą urzędnik jest obowiązany zwrócić się do operatora telekomunikacyjnego o udzielenie mu danych na temat ruchu w sieci. Rzecznik ds. Informacji może sprawować nadzór po tym jak żądanie danych miało już miejsce, ale urzędnik prowadzący dochodzenie musi w każdej sytuacji jedynie uzasadnić żądanie urzędnika wyższego szczebla. Pod koniec 2002 r. BBC

¹⁴³ Stanley, J. (2004) *The Surveillance-Industrial Complex [Połączenie przemysłu z nadzorem]*, Washington DC: ACLU. http://www.aclu.org/FilesPDFs/surveillance_report.pdf

¹⁴⁴ Aby zapoznać się z szeroko zakrojoną dyskusją na te tematy oraz FIP, zob.: Tavani (1999) *op cit.* n.60.

donosiło, że organy egzekwujące prawo zwróciły się do operatorów sieci telefonii komórkowej z wnioskiem o przekazanie im danych dotyczących ruchu w sieci ponad 400 000 razy.¹⁴⁵ Co się zaś tyczy organów ścigania, utrzymywanie, że aparat komórkowy nie ma żadnego związku z użytkownikiem i że gromadzenie oraz przetwarzanie pseudo-danych dotyczących ruchu nie miało wpływu na ochronę danych, wydaje się nieuzasadnione.

11.2.12. Podczas gdy ustawodawstwo dotyczące prywatności zmniejsza niektóre obawy związane z nadzorem konsumenckim, wykorzystanie jego skoncentrowanych na jednostce ukrytych technik przetwarzania informacji oznacza, że kategorie społeczne i ich skutki są ukrywane przed tymi, których bezpośrednio dotyczą. Prawdziwa kontrola informacji wymaga większej przejrzystości organizacyjnej w odniesieniu do gromadzenia danych i przetwarzania informacji, jak również jasnych wskazówek wyjaśniających, w których momencie naruszone zostaje bezpieczeństwo danych osobowych. Problem stwarza pogodzenie tej przejrzystości z zapotrzebowaniem na wysoce konkurencyjną gospodarkę, w której przejrzystość może w rzeczywistości osłabiać korzyści wynikające z organizacji przetwarzania danych. Jeśli nie zostanie to zrównoważone, czy to za pomocą systemów regulacyjnych czy też etycznych praktyk korporacyjnych dotyczących przejrzystości, pozostanie obawa, że nadzór konsumencki nadal będzie umacniał i pogłębiał podziały oraz selekcję, które są nieetyczne w myśl zasad demokracji. Nadzór konsumencki może zatem przybrać na sile, skoro „sortowanie cybernetyczne” dokonujące podziałów wśród konsumentów opiera się na ich zakładanej wartości gospodarczej oraz politycznej zamiast na ich inicjatywie i samostanowieniu.¹⁴⁶

11.3. Wybór i zgoda

11.3.1. Kolejny problem dotyczy wyboru i zgody. Wybór był jednym z ważnych przedmiotów debat poświęconych nadzorowi i ochronie danych w Ameryce Północnej. Jednakże w Zjednoczonym Królestwie, w porównaniu z innymi środkami ochrony, zajmuje raczej niższą pozycję.

11.3.2. W medycynie istnieje kilka form wyrażania zgody: zgoda na leczenie, zgoda na przekazanie informacji i zgoda na wykorzystanie informacji medycznych dotyczących poszczególnych osób w badaniach medycznych. Kluczowym pytaniem we wszystkich przypadkach jest to, jakie informacje zostały dostarczone danej osobie w celu umożliwienia jej podjęcia decyzji. „Świadoma zgoda pacjenta” na wykorzystanie danych osobowych jest wymagana między innymi ze względu na fakt ogromnych nadużyć w zakresie etyki medycznej, jakiej dopuszczono się w obozach koncentracyjnych podczas drugiej wojny światowej. W przypadku gdy pacjenci są proszeni o przekazanie informacji do dużych badawczych baz danych należy zadać pytanie, czy możliwe jest przewidzenie wszystkich potencjalnych celów wykorzystywania takich danych i czy w przyszłości może zachodzić potrzeba ponownego udzielenia zgody. W związku z powyższym konieczne jest niekiedy spełnienie dodatkowego wymogu, aby dane gromadzone do celów medycznych (w tym do celów badań medycznych) były wykorzystywane wyłącznie w tych celach, w jakich zostały pierwotnie zgromadzone. Każde nowe wykorzystanie wymaga, aby każdy pacjent otrzymał odpowiednie informacje i podpisał nową zgodę.

¹⁴⁵ Zob. n.80.

¹⁴⁶ Co jest rozumiane jako „sortowanie panoptyczne” opisane szczegółowo w: Gandy (1993) *op cit.* n. 24.

11.3.3. Problem wyboru i zgody może zostać zobrazowany za pomocą następującego przykładu: czy dana osoba może wybrać, czy chce lub nie poddać się obserwacji, jeżeli jednocześnie chce prowadzić normalne życie? Jak można w ogóle utrzymywać, że wyraziliśmy zgodę na objęcie nadzorem? Problem zgody jest również powszechnie obecny w systemie sądownictwa karnego. Nie wyrażamy zgody na monitorowanie nas przez system CCTV, kiedy przebywamy w miejscach publicznych, nikt też nie wyraził zgody na rejestrowanie przemieszczeń jego samochodu w centrali ANPR ACPO. Osoby zatrzymane nie wyrażają odpowiedniej zgody, a mimo to zostają im pobrane odciski palców i próbki DNA, które następnie są stale przechowywane w policyjnej krajowej bazie danych, nawet jeśli osoby te zostały zwolnione bez postawienia im zarzutów. Lecz o ile dana osoba nie może zostać zmuszona do oddania próbki moczu w celu przebadania jej na obecność narkotyków, o tyle w takiej sytuacji nie ma większego wyboru, gdyż odmowa może wiązać się z karą grzywny, pozbawienia wolności lub obiema karami. Jest rzeczą prawie niemożliwą, aby dana osoba dowiedziała się, w jaki sposób wykorzystywane są informacje oraz w jak subtelny sposób może mieć to wpływ na jej życie; na przykład poprzez zwiększenie prawdopodobieństwa zatrzymania jej samochodu przez policję lub żądanie, aby z góry płaciła za towary i usługi.

11.3.4. Rozwiązaniem tego problemu mogłoby być uczynienie współpracy obywateli z nadzorem państwowym nieobowiązkową w przypadkach, gdy jest to możliwe, co zostało zaproponowane w odniesieniu do dowodów osobistych w Wielkiej Brytanii. Jednakże jest to w dużej mierze rozwiązanie iluzoryczne, gdyż o ile okaże się, że dowód osobisty jest wymagany do uzyskania dostępu do pewnych usług, stanie się on *de facto* obowiązkowy. Ponadto istniejące dokumenty potwierdzające tożsamość odnoszą się do pojedynczych ról pełnionych przez obywateli takich jak rola kierowcy, konsumenta czy turysty, podczas gdy system dowodów osobistych pozwala rządowi monitorować działania realizowane w ramach różnych ról, jak te wyżej wymienione, a także w ramach roli obywatela.

11.3.5. Jeśli chodzi o miejsce pracy, udzielanie zgody również nie jest prostą sprawą. W różnych krajach istnieją różne opinie i toczą się debaty dotyczące tego, czy organizacje powinny informować w sposób ogólny pracowników o tym, że mogą znajdować się pod stałym nadzorem, czy też nie jest to wymagane. W Australii na przykład pracodawcy muszą uzyskać zezwolenie sądu pokoju, aby prowadzić potajemną obserwację swoich pracowników. W Zjednoczonym Królestwie z Ustawy o uprawnieniach śledczych (RIPA) z 2000 r. wynika, że jeżeli dane przedsiębiorstwo działa w celu ochrony „prawnie uzasadnionego interesu”, może ono potajemnie przejmować wiadomości wysyłane przez pracownika, chociaż musi jednocześnie spełniać wymogi Ustawy o ochronie danych osobowych. Jeśli chodzi na przykład o metodę kontroli *mystery shopping*, opinie są podzielone; z jednej strony uważa się, że takie praktyki są nieetyczne ze względu na stopień zakamuflowania, narażanie na ujawnienie i brak odpowiedniej zgody.¹⁴⁷ Według innych, pracodawcy muszą przedstawić swoim pracownikom wyniki takiej kontroli w celu uświadomienia im faktu jej przeprowadzania w taki sposób, który nie ujawni samego mechanizmu kontroli.¹⁴⁸

11.4. Dyskryminacja: szybkość, dostęp i wyłączenie społeczne

¹⁴⁷ Shing, M.N.K. and Spence, L. (2002) „The limits of competitive intelligence: is mystery shopping ethical? [Granice wywiadu konkurencyjnego: czy kontrole typu mystery shopping są etyczne?]" *Business Ethics: A European Review* 11(4):343-353.

¹⁴⁸ Wilson, A.M. (2001) „Mystery shopping: using deception to measure service performance [Mystery shopping: stosowanie podstępu w celu zmierzenia jakości usług]", *Psychology and Marketing* 18(7); 721-734.

11.4.1. Dyskryminacja przejawiająca się różnicami w szybkości i łatwości dostępu oraz różnymi stopniami wyłączenia społecznego jest głównym skutkiem procesu selekcji społecznej wynikającym z nadzoru. Obecnie stara biurokratyczna logika administracji rządowej próbuje wykorzystywać zarówno biometryczne, jak i sieciowe systemy identyfikacji, dążąc do stworzenia świata pełnego różnorodnych tożsamości i dokumentów je potwierdzających. W świecie tym jednostki posiadające dostęp do zasobów to wysoce mobilni, międzynarodowi biznesmeni, turyści i podobne osoby, a ich systemy identyfikacji (począwszy od kart kredytowych po karty lojalnościowe klientów linii lotniczych) wydają się jeszcze bardziej zwiększać łatwość ich przemieszczania się. Jednakże dla innych osób, które pracują (lub co gorsza są bezrobotne), migrantów, uchodźców lub osób ubiegających się o azyl, nie mówiąc o osobach o charakterystycznych, muzułmańsko lub arabsko brzmiących nazwiskach, systemy te ograniczają ich mobilność zarówno w granicach krajów, jak i pomiędzy nimi.

11.4.2. Logika rządowa uległa zmianie. Podczas gdy dawne, dwudziestowieczne rozumienie pojęcia obywatelstwo kładło główny nacisk na *włączenie* wszystkich kwalifikujących się osób do systemów opieki zdrowotnej, opieki społecznej i ochrony prawnej, nowsze praktyki, w tym systemy dokumentów tożsamości, wydają się podkreślać *wyłączenie* niepożądanego elementu.¹⁴⁹ Kluczowe wydarzenia, których symboliczną (choć nie historyczną) datą rozpoczęcia był dzień 11 września, przyczyniły się do szybkiego rozwoju nowych systemów identyfikacji i nadzoru.¹⁵⁰ Problem polega na tym, że ludzie przemieszczają się z różnych powodów, w związku z czym pożądane są takie systemy identyfikacji, które pozwolą na ich klasyfikację nie tylko ze względu na obywatelstwo, ale również na ich status, tj. czasowy, stały, narodowy itd. Bazy danych wyposażone w funkcję wyszukiwania pozwalają już na tego typu klasyfikację i kategoryzację społeczną.

11.4.3. Zwiększenie kontroli życia miejskiego wywołało potężny proces wykluczenia społecznego. Przejawia się on głównie odrzuceniem ludzi i miejsc postrzeganych jako niekorzystne lub ryzykowne. Wówczas przede wszystkim nowe technologie nadzoru mogą znacznie spowolnić tempo życia niektórych osób, stwarzając w ten sposób dodatkowe logistyczne utrudnienia. Znaczna część tej społecznej selekcji za pomocą systemów nadzoru odbywa się automatycznie (tj. bez udziału człowieka), stale (tj. 24 godziny na dobę) i w czasie rzeczywistym (tj. bez opóźnień) dzięki odpowiedniemu oprogramowaniu. Bardzo często motywacja pozwala przewyżczać bariery elektroniczne i fizyczne, jakie dotyczą wpływowych uprzywilejowanych i potężnych ludzi lub występują w określonych miejscach, podczas gdy stają oni przed wyzwaniem związanym z życiem i działaniem w gęsto zaludnionych, miejskich i coraz bardziej mobilnych społeczeństwach, które wysoko cenią połączenia sieciowe i przepływy informacji umożliwiające łączenie się z innymi miejscami.¹⁵¹ Jednakże po wprowadzeniu zarówno dostępu, jak i blokady są one coraz bardziej automatycznie¹⁵² kontrolowane, co stwarza zagrożenie

¹⁴⁹ Bigo, D. (2004) „Globalized in-security: the field of the professionals of unease management and the ban-opticon [Globalne bezpieczeństwo wewnętrzne: pole działania specjalistów w zakresie zarządzania niepokojem społecznym a monitoring doskonały]”, *Traces*, 4.

¹⁵⁰ Lyon, D. (2003) *op cit.* n.6; Ball, K. and Webster, F. (eds.) „*The Intensification of Surveillance [Intensyfikacja nadzoru]*”, London: Pluto Press.

¹⁵¹ Andrejevic, M. (2003) „Monitored mobility in the era of mass customization [Monitorowana mobilność w dobie masowej indywidualizacji]”, *Space and Culture*, 6: 132-150.

¹⁵² Lianos, M. (2001) *op cit.* n.109; Lianos, M. (2003) „Social control after Foucault [Kontrola społeczna po Foucault]” *Surveillance & Society* 1(3): 412-430. [http://www.surveillance-and-society.org/articles1\(3\)/AfterFoucault.pdf](http://www.surveillance-and-society.org/articles1(3)/AfterFoucault.pdf).

jeszcze bardziej zdecydowanego podziału technologicznego współczesnego społeczeństwa na klasy szybkie, bardzo mobilne i korzystające z połączeń oraz klasy powolne, o niskiej mobilności i nie korzystające z połączeń.

11.4.4. Taki podział może na stałe zakorzenić się w strukturze społecznej. Zaobserwowaliśmy, że usprawniona odprawa graniczna może znacznie przyspieszyć podróże członków płatnych programów lojalnościowych pasażerów. W miastach, oceny sytuacji ekonomicznej dokonywane w oparciu o ciągle związki z rejestrami kredytowymi i innymi tego typu rejestrami, mogłyby doprowadzić do regularnego wykluczania i piętnowania osób o gorszej sytuacji materialnej z coraz bardziej skomercjalizowanych miast i centrów miejskich o rosnącym statusie. Algorytmiczne systemy CCTV mogą zakorzenić źródła uprzedzeń społecznych w oprogramowaniu, na którym opiera się ich działanie. Wraz z rosnącą likwidacją funkcji operatorów kamer głównym elementem regulacyjnym staje się kod stosowany w oprogramowaniu, „decydujący” o tym, jakie zachowanie, wygląd zewnętrzny, twarz i inne wyznaczniki mogą gwarantować przeprowadzenie pewnych działań kontroli lub wykluczenia z populacji miasta lub danego narodu. Systemy dowodów tożsamości również pozwalają na subtelną klasyfikację populacji na podstawie niejasnych kryteriów wypaczających system na niekorzyść tych, którzy już i tak znajdują się w trudnej pozycji. Tego rodzaju selekcja społeczna przyczynia się do powstania obywatelstwa drugiej klasy. W sytuacji, gdy tożsamość kulturowa i narodowa stały się tak trudnym wymiarem życia obciążonym ciężkim ładunkiem życiowych szans i wyborów, wspomnień i pragnień, paradoksalne jest to, że jednocześnie dąży się do zredukowania tego wymiaru do wzorów komputerowych i algorytmów w celu ułatwienia procedur biurokratycznych, policyjnych i związanych z administracją przedsiębiorstw.

11.4.5. Wyłączenie przejawia się również w strukturze cen towarów. Sprawa Amazon.com, która sprzedawała DVD różnym klientom po różnych cenach wywołała pytanie czy może zachodzić konieczność interwencji prawodawczej w celu zapewnienia, że nie nastąpi masowe ustalenie poziomu cen handlowych na przykład w oparciu o działanie automatycznego nadzoru RFID. Konsumenci stają się coraz bardziej narażeni na wykorzystywanie informacji dotyczących ich sytuacji ekonomicznej. Ogromna zależność od konkretnych technologii i poszczególnych numerów lub kodów identyfikacyjnych stwarza pole do nadużyć i wyzysku informacji. Ciągłe innowacje w przetwarzaniu danych i zwiększone gromadzenie różnych rodzajów danych doprowadziło do upowszechnienia praktyk selekcji społecznej, co wiąże się z niebezpieczeństwem dyskryminacji i wykluczenia.

11.4.6. Podczas gdy trudno jest wyciągać wnioski dotyczące nadzoru i wyłączenia społecznego w miejscu pracy głównie ze względu na istniejące zawodowe i społeczne wyznaczniki rynku pracy, jednym z obszarów działania nadzoru w miejscu pracy jest rozwarstwianie możliwości zatrudnienia: e-rekrutacja. Przeglądanie wielu CV i poszukiwanie potencjalnych kandydatów podnosi dwa rodzaje pytań o dyskryminację. Po pierwsze e-rekrutacja jest procesem subiektywnym podlegającym „regułom kciuka” podobnym do tych stosowanych przez osoby rekrutujące stojące przed wyborem pomiędzy różnymi kandydatami.¹⁵³ Wyszukiwanie według słów kluczowych jest obecnie rutynowo stosowanym narzędziem selekcji, a ponieważ stosowanie różnych słów kluczowych różni się w zależności od rekrutującego, może ono dawać

¹⁵³ Tversky, A. and Kahneman, D (1974) „Judgement under uncertainty: heuristics and biases [Osąd w niepewności: heurystyka i uprzedzenia]” *Science* 185(4157): 1124-1131

różne wyniki.¹⁵⁴ O ile sprawą dyskusyjną jest to, czy pozyskiwanie pożądaných wyników za pomocą określonych słów kluczowych stanowi o doświadczeniu zawodowym i wiedzy rekrutującego, to na pewno odzwierciedla ono jego własne uprzedzenia. Problem staje się jeszcze bardziej złożony, jeżeli uświadomimy sobie, że kandydaci posiadają różne umiejętności w zakresie pisania CV. Wykorzystywanie standardowych formularzy może w jakiś sposób rozwiązywać ten problem, podobnie jak ma to miejsce w przypadku stosowania całych wyrażen w wyszukiwaniu kwalifikacji, a także ścisłego przestrzegania zasad polityki w praktyce.

11.4.7. Po drugie, e-rekrutacja jest dyskryminacyjna, gdyż pewne grupy społeczne, ekonomiczne i etniczne nie dysponują łatwym dostępem do Internetu. Dlatego też koncentracja na e-rekrutacji przyczynia się do skutecznego wykluczenia tych grup z całości rynku pracy. O ile obecnie znacznie rozwinęło się wiele niszowych stron internetowych, pierwotnie były one kierowane go białych mężczyzn należących do klasy średniej, zatrudnionych w sektorze technicznym i IT.¹⁵⁵ Wśród firm obserwuje się silną tendencję do standaryzacji i formalizacji procesów e-rekrutacji, co raczej zapewni dopływ "takich samych" kandydatów niż przyczyni się do ich dywersyfikacji. Marconi Capital zrewidował swoją strategię e-rekrutacji po tym jak dostrzeżono, że nie przyciągała ona etnicznej czy rasowej mieszanki ludzi, których firma chciała zatrudnić, zaobserwowano również, że kobiety często rezygnowały z internetowych procedur rekrutacji ze względu na ich bezosobowy charakter.¹⁵⁶ Brytyjska komisja praw osób niepełnosprawnych zbadała 1000 stron internetowych i stwierdziła, że 81% nie spełniała najbardziej podstawowych wytycznych w zakresie dostępności, co oznacza, że osiem na dziesięć stron internetowych w Zjednoczonym Królestwie wyklucza z ubiegania się o pracę za pośrednictwem Internetu 1,3 miliona osób w wieku aktywności zawodowej.¹⁵⁷ Świadome stosowanie zróżnicowanych kanałów rekrutacyjnych, zamieszczanie ogłoszeń na różnych stronach internetowych i spełnianie wymogów w zakresie różnorodności są kluczowymi krokami, jakie powinny poczynić organizacje.

11.4.8. Paradoksalnie, jak już zostało wspomniane we Wprowadzeniu, znaczna część nadzoru jest ukierunkowana na włączanie, począwszy od podstawowych mechanizmów państwa opiekuńczego, a ideologia „bezpieczeństwo przede wszystkim” tylko zwiększyła to zjawisko. Kluczowym przykładem jest ogromny rozwój polityki na rzecz zapewnienia bezpieczeństwa dzieci w sposób wszechstronny i zapobiegawczy. Dotyczy to również wspierania wysiłków mających na celu zwalczanie wykluczenia społecznego oraz, w szczególności, interwencje w sektorze edukacji. Oznacza to przyjęcie nowych punktów wyjścia, takich jak baza danych dzieci lub „wykaz wspólnych informacji” obejmujący 150 obszarów lokalnych, który będzie obejmował dane dotyczące wszystkich dzieci w Anglii i Walii do 18. roku życia. Ich cel jest szerszy niż ochrona dzieci i mają one pełnić bardziej holistyczną rolę związaną z zapewnieniem dzieciom opieki oraz określonych usług: odpowiednie wskaźniki będą identyfikować każde dziecko i wskazywać, czy zostały mu zapewnione

¹⁵⁴ Mohamed, A.A., Orife, J. and Wibowo, K. (2002) „The legality of key word search as a personnel selection tool [Legalność wyszukiwania według hasła jako narzędzia stosowanego w naborze pracowników]” *Employee Relations* 24(5).

¹⁵⁵ Sharf, J. (2000) „As if g-loaded adverse impact isn't bad enough, internet recruiters can be expected to be accused of 'e-loaded' impact [Jeśli niekorzystne skutki testowania inteligencji nie są wystarczająco szkodliwe, osoby odpowiedzialne za internetową rekrutację mogą spodziewać się oskarżeń o nadmierne wykorzystywanie e-technologii]”, *The Industrial-Organizational Psychologist* 38:156.

¹⁵⁶ Smethurst, S. (2004) „The allure of online [Urok Internetu]” *People Management* 10(15): 38 – 40; Czerny, A. (2004) „Log on turn off for women [Zamknięcie Internetu na kobiety]”, *People Management* 10(15): 10.

¹⁵⁷ Smethurst (2004) *op cit.*

właściwe usługi. Baza danych powinna zawierać podstawowe informacje plus indywidualne numery identyfikacyjne oraz dane kontaktowe rodziców, szkół, przedstawicieli służby zdrowia i innych specjalistów spełniających dodatkowe potrzeby, którzy mogą dysponować ważnymi informacjami i ocenami. Pomyśl ten, który został szeroko omówiony w Zielonej Księdze z 2003 r. *Liczy się każde dziecko*¹⁵⁸ i przyjęty w Ustawie o dzieciach z 2004 r., ma na celu nie tylko zapobieżenie przyszłym tragediom, ale również realizację o wiele bogatszego planu opieki mającego na celu zaspokojenie potrzeb dzieci, a więc nawiązującego również do edukacji i opieki zdrowotnej.

11.5. *Demokracja, odpowiedzialność i przejrzystość*

11.5.1. W tym miejscu należy zadać wiele ważnych pytań: jakie są granice kontroli publicznej? W jaki sposób powinna być regulowana granica pomiędzy komercyjnymi bazami danych a kontrolą publiczną i państwową? W jaki sposób prywatne firmy będą odpowiadały za błędy występujące w ich systemach baz danych? Obecnie bardzo ogranicza się dostęp obywatelom, którzy znaleźli się na liście kontrolnej „inteligentnej granicy”. Podczas gdy wiele agencji lub organów może korzystać z dostępu do systemu lub umieszczać w nim informacje, to możliwości w zakresie usuwania lub sprostowania danych są bardzo ograniczone. Ponadto istnieją ważne pytania dotyczące odpowiedzialności wybranych rządów przed ich obywatelami oraz zagranicznego charakteru wielu prywatnych dostawców współczesnych systemów nadzoru. W związku z tym komercyjne źródła danych takie jak transakcje przy użyciu karty kredytowej lub zapisy rozmów przez telefon komórkowy jakie są przeprowadzane przez koncerny międzynarodowe mogą mieć charakter zagraniczny i pozostawać poza zasięgiem jurysdykcji politycznej. Ostatnie przykłady przekazania informacji przez koncerny międzynarodowe mogą stanowić spore wyzwanie dla kontroli i regulacji publicznych, zwłaszcza w przypadku gdy dana firma jest posiadaczem danych komercyjnych i zawarła umowę o świadczenie usług w zakresie nadzoru.

11.5.2. Szczególnie trudne jest ustanowienie odpowiedniej polityki w zakresie tajnego nadzoru. Jeżeli dotyczy to szpiegostwa międzynarodowego, jak ma to miejsce w przypadku systemu ECHELON, fakt, że takie systemy oficjalnie "nie istnieją" lub że funkcjonują poza prawem, albo są prowadzone we współpracy z agencjami innych państw, wystawia na pośmiewisko idee wyboru i zgody. Zjednoczone Królestwo ma długą tradycję działalności wywiadowczej i zakłada ogólne wyłączenie służb specjalnych spod obowiązującego prawa. Na przykład Ustawa o służbach wywiadowczych (ISA) z 1994 r. zezwoliła GCHQ na „monitorowanie lub ingerowanie w emisje elektromagnetyczne, akustyczne i inne, a także w zakresie sprzętu służącego do wytwarzania takich emisji oraz do pozyskiwania i dostarczania informacji pochodzących z takich emisji lub sprzętu lub ich dotyczących oraz zaszyfrowanego materiału” w różnych celach „w interesie bezpieczeństwa krajowego [...] dobrobytu Zjednoczonego Królestwa [lub] w ramach wsparcia na rzecz zapobieżenia poważnym przestępstwom lub w celu ich wykrycia”¹⁵⁹.

11.5.3. Powszechnie uważa się, że każdy konkretny przypadek inwigilacji za pomocą sieci telekomunikacyjnej (podśluch telefoniczny) wymaga odpowiedniego nakazu. Jest tak w przypadku zwykłego nadzoru policyjnego.

¹⁵⁸ Chief Secretary to the Treasury (2003) „*Every Child Matters [Liczy się każde dziecko]*” (Cm 5860), London: The Stationary Office. http://www.everychildmatters.gov.uk/_files/EBE7EEAC90382663E0D5BBF24C99A7AC.pdf.

¹⁵⁹ Intelligence Services Act [Ustawa o służbach wywiadowczych] 1994, Rozdział 13, Sekcja 3, London: HMSO.

Jednakże jeden szczególnie zmyślnie sformułowany ustęp ISA stanowi, że „żaden przypadek wkroczenia lub zajęcia własności, lub też ingerencji w komunikację bezprzewodową nie jest bezprawny, jeżeli ma on miejsce na podstawie nakazu wydanego przez sekretarza stanu na mocy niniejszej sekcji”¹⁶⁰, jednakże nie stanowi, że każde z takich działań jest bezprawne, *chyba że* odbywa się ono na podstawie nakazu. W rozumieniu Ustawy „wkroczenie lub ingerencja we własność lub w telegrafię bezprzewodową” może odbyć się zgodnie z prawem bez odpowiedniego nakazu.

11.5.4. W innych krajach nadzór i w szczególności wymiana informacji państwowych były niejednokrotnie surowo krytykowane przez organy kontroli i środki przekazu. Być może najsłynniejszym tego przykładem była baza danych kanadyjskiego rządu Longitudinal Labour Force File zawierające ogromną ilość danych federalnych i prowincjonalnych dotyczących obywateli kanadyjskich, w tym informacje w zakresie opieki społecznej, podatku dochodowego, imigracji, służb zatrudnienia i ubezpieczenia od bezrobocia. Około 2000 informacji dotyczących około 34 milionów Kanadyjczyków zostało uwikłanych w ten mało widoczny, słabo uregulowany program badawczy dotyczący służb publicznych. Ujawnienie tego proceduru wywołało w 2000 r. fale protestów i podjęcie zdecydowanych działań przez federalnego rzecznika ds. prywatności na rzecz wzmocnienia ochrony prywatności, w tym konieczności szyfrowania i anonimizacji, a także zwiększenia odpowiedzialności i przejrzystości, które powinny zostać uwzględnione w przyszłych przypadkach wymiany informacji.¹⁶¹ W Japonii w 2002 r. wybuchł wielki skandal po tym, jak okazało się, że Agencja Obrony gromadziła tajną dokumentację dotyczącą osób, które chciały uzyskać informacje na swój temat, a Siły Samoobrony gromadziły systematycznie dane dotyczące osób, które występowały z wnioskami o ujawnienie informacji, w tym w zakresie zatrudnienia, miejsca pracy i ewentualnych powiązań z pracownikami SDF¹⁶².

11.5.5. Na mocy obowiązującego ustawodawstwa obywatele wielu krajów mają prawo wiedzieć, jakie informacje ich dotyczące są gromadzone oraz w jaki sposób są one wykorzystywane, chociaż istnieje kilka wyjątków od tego wymogu. Zgodnie z tym prawem wymaga się istnienia „administratora danych” w celu dostarczania każdej osobie informacji o wszelkich dotyczących jej danych, jakie są przechowywane oraz o wszelkim przetwarzaniu, jakemu są poddawane takie dane. Taki wymóg może w pewien sposób skorygować asymetrię potęgi nadzoru, zwłaszcza gdy zgoda na wykorzystanie naszych danych osobowych została raczej wymuszona niż przez nas udzielona. Jednakże wiele osób nie zna swoich praw, nie korzysta z nich i uzyskuje w tym zakresie niewiele pomocy od osób trzecich.

11.5.6. Intensywna infogilacja staje się normalnym zjawiskiem w nowoczesnym państwie i sama w sobie może być możliwa do uzasadnienia i uzasadniona przez osoby popierające tego typu działania w interesie publicznym. Takie działania mogą być czasami realizowane za zgodą parlamentu. Działania te są utrudnione ze względu na manipulowanie ogromnymi ilościami danych przekraczającymi granice ustalone zgodnie z zasadami i przepisami w zakresie

¹⁶⁰ Intelligence Services Act [Ustawa o służbach wywiadowczych] 1994, Rozdział 13, Sekcja 5, London: HMSO.

¹⁶¹ Todd, D. (2001) „*Politicizing Privacy: 'Focusing Events' and the Dynamics of Conflict* [Upolitycznianie prywatności: główne wydarzenia i dynamika konfliktu]”. Nieopublikowana praca magisterska, University of Victoria, BC, Canada, 58-86; zob.: HRDC Canada (2000) „HRDC dismantles longitudinal labour force file databank [HRDC rozwiązuje bazę danych longitudinal labour force file]”, dnia 29 maja, http://www.hrsdc.gc.ca/en/cs/comm/news/2000/000529_e.shtml.

¹⁶² Abe, K. (2004) „Everyday policing in Japan: surveillance, media, government and public opinion [Codzienne pilnowanie porządku w Japonii: nadzór, media, opinia rządowa i publiczna]” *International Sociology*, 19: 215-231.

ochrony danych (parlament) oraz inne wymogi i wytyczne dotyczące tego, w jaki sposób informacje powinny być gromadzone, segregowane i przekazywane. Możemy przyzwyczaić się do bycia pod nadzorem, do śledzenia lub nawet przewidywania naszych czynności i przemieszczeń w sposób dla nas niezauważalny, zwłaszcza jeśli chodzi o służby publiczne, bez możliwości opowiedzenia się za lub przeciw lub pełnego zrozumienia, co dzieje się z naszymi danymi. Możemy uznać te ograniczenia prywatności za „uzasadnione” albo odrzucić je, biorąc pod uwagę, co powinno oznaczać bycie obywatelem. Jest mało prawdopodobne, że sytuacja polityczna pozwoli w końcu powołać się na prawa dotyczące prywatności, aby sprzeciwić się żądaniom organizacji rządowych stawianym w „interesie publicznym”, nawet wtedy, gdy ten interes wydaje się być jasny i mieć ogromne znaczenie. Jeżeli nadzór miałby być „proporcjonalny”, to wiele zależy od sposobu interpretacji tego terminu oraz tego, kto dokonuje takiej interpretacji. Ponadto dużo zależy od zabezpieczeń, z jakimi wiąże się te nowe, intruzyjne praktyki.

- 11.5.7. Jednakże wspierając nowe plany i programy, rząd od czasu do czasu podnosił również problem prywatności i zagrożeń, jakie ze sobą niesie nadzór. Dlatego też próbował poruszyć ważne pytanie o zaufanie publiczne w procesach informacyjnych "rządu doby informacji", w tym w zakresie świadczenia usług zarówno za pośrednictwem Internetu, jak i innych metod. Czasami „aspekty ujemne” nie zostały uwzględnione w takim stopniu jak przewidywane korzyści. Jednakże kwestie dotyczące prywatności zajmowały wysoką pozycję w debatach poświęconych zaufaniu, chociaż nie była ona tak znacząca ani tak wpływowa jak oczekiwały tego osoby zaniepokojone potencjalnym nadzorem, z jakim mogły się wiązać nowe, bardziej zintegrowane i rozległe wykorzystania baz danych i podobnych źródeł. Kiedy Jednostka ds. Wyników i Innowacji wydała swój raport w 2002 r. dotyczący prywatności i wymiany danych,¹⁶³ poczyniła próby w celu zapewnienia rozwiązań, które jednocześnie pozwoliłyby na wykorzystywanie i wymianę danych osobowych oraz zwiększyłyby ochronę prywatności. Jednakże zastosowanie tych zaleceń w praktyce w znacznej części nie powiodło się ze względu na zaistniałe wydarzenia i nowe inicjatywy, dzięki którym perspektywy dobrej ochrony prywatności w sektorze usług publicznych sprawiają wrażenie odległych, chyba że inicjatywy te można uzupełnić o zabezpieczenia wyrównujące lub wdrożyć je po realizacji inicjatyw.

¹⁶³ Cabinet Office Performance and Innovation Unit (PIU) (2002) „*Privacy and Data-Sharing: The Way Forward for Public Services*.” [Prywatność a wymiana danych: Rozwiązanie dla służb publicznych]” London: Cabinet Office.

Część C/1:
Tydzień z życia
w społeczeństwie nadzorowanym w 2006 r.

12. Wprowadzenie

- 12.1. Jest Londyn 2006 r. Rodzina Jonesów wraca z wakacji na Florydzie. Ojciec, Gareth, jest kierownikiem w call centre, a matka Yasmin jest pracownikiem społecznym. Yasmin pochodzi z Pakistanu i posiada podwójne obywatelstwo. Towarzyszy im jej posiadająca pakistański paszport matka Geeta oraz trójka ich dzieci, 18-letni Ben, 14-letnia Sara i 10-letni Toby.
- 12.2. Członkowie rodziny Jonesów są obywatelami społeczeństwa nadzorowanego. Przez cały tydzień od ich powrotu, czasem bezwiednie, a czasem przy ich pełnej wiedzy, systemy nadzoru wpływają na ich życie i kształtują je. Na kolejnych stronach pokażemy w jaki sposób ich codzienne zajęcia są teraz osadzone w systemach nadzoru oraz w jaki sposób nadzór wpływa na ich działania i relacje.

13. Na lotnisku

- 13.1. Chociaż rodzinne wakacje dobiegły końca i Jonesowie są w drodze do domu, Gareth Jones jest z siebie zadowolony. To on sfinansował wakacje. Jako kierownik regionalny Sentasi, najszybciej rozwijającej się sieci call centre, dostał pokaźną premię za wyniki za swój udział w otwieraniu nowych biur w Hyderabad¹⁶⁴. Wyróżnił się komunikatywną znajomością urdu będącą wynikiem dwudziestoletniego małżeństwa z Yasmin. Dzięki premii mógł opłacić wakacje swojego życia: trzy tygodnie na Florydzie, zwiedzanie Walt Disney World, Florida Keys i obserwowanie wielorybów. Biorąc pod uwagę, że Ben w przyszłym roku pójdzie na studia (o ile poprawi ocenę z jednego przedmiotu z poziomu A, z którego brał dodatkowe lekcje w szkole), mogły to być ostatnie wakacje z udziałem całej rodziny. Poza tym Yasmin naprawdę potrzebowała odpoczynku. Po tym jak Toby, ich najmłodszy syn, zaczął szkołę Yasmin podjęła szkolenie na pracownika społecznego, które zaliczyła celująco, a następnie otrzymała ofertę pracy w międzyresortowym zespole ds. przestępczości wśród nieletnich. Od ich ostatnich porządných wakacji minęły już cztery lata. Gareth cieszył się z tego, że matka Yasmin, Geeta również im towarzyszyła; to takie małe podziękowanie za wsparcie finansowe jakiego im udzielała w ciągu ostatnich lat. Cieszył się również z towarzystwa Geety ze względu na specjalną więź łączącą ją z Sarą, jak to często bywa między babcią i wnuczką, co pozwoliło w pewnym stopniu uspokoić wybuchowy temperament nastolatki. Gareth miał coraz większe trudności z dotarciem do córki. Wiedział, że opuszczała lekcje i obwiniał za to towarzystwo, z którym się trzymała; ona nazywała ich „Gotami”. On uważał, że są makabryczni: ubrani na czarno, z poфарbowanymi na czarno włosami, buty z ćwiekami i z kolczykami na całym ciele. Zmusił ją do wyjęcia kolczyka z języka, ale w końcu ustąpił w przypadku licznych kolczyków w uszach. Młódzież!
- 13.2. Czekając w kolejce ma nadzieję, że nie spotkają ich problemy podobne do tych, jakich doświadczyli podczas odprawy w Gatwick. Po minięciu ochrony cała rodzina została poproszona na bok, ich bagaż został nie tylko prześwietlony, ale również

¹⁶⁴ Wszystkie nazwiska osób prywatnych i nazwy firm są fikcyjne. Odpowiedniki ze świata rzeczywistego zostały opisane w przypisach.

dokładnie przeszukany ręcznie, a oni musieli odpowiedzieć na liczne pytania dotyczące ich ostatniej międzynarodowej podróży. Procedura zajęła ponad pół godziny, po czym mogli dalej uczestniczyć w odprawie. Powiedziano im, że zostali wybrani losowo w ramach aktualnie obowiązujących dodatkowych środków bezpieczeństwa. Jednakże Gareth podejrzewał, że zostali wybrani ze względu na pakistańskie obywatelstwo jego żony i teściowej.¹⁶⁵

13.3. Zastanawiając się, czy to samo przydarzy im się w drodze powrotnej, Gareth kładzie swój bagaż podręczny na taśmociągu bagażowym wraz z kluczami, drobnymi, kurtką i butami umieszczonymi w koszyku, przechodzi przez bramkę i odczuwa ulgę, gdyż nie uruchomił alarmu. Jednakże w stanowisku obok, do którego zostały skierowane kobiety, obserwuje z pewnym zażenowaniem jak jego córka zdejmuje buty, obrożę, wielki czarny pasek i kurtkę nabitą ćwiekami i nawet wtedy, częściowo rozebrana, wciąż uruchamia dzwonek przechodząc przez bramkę. Każą jej przejść po raz kolejny i po tym jak po raz kolejny uruchamia alarm zostaje zabrana do małej zasłoniętej kabiny, gdzie zostaje poddana dokładnej kontroli osobistej przez strażniczkę zanim zostanie będzie mogła kontynuować procedurę. Po przejściu kontroli zostają ponownie zmuszeni do czekania w kolejce w celu sfotografowania ich i pobrania odcisków palców, podobnie jak wtedy, gdy trzy tygodnie temu lecieli do Stanów Zjednoczonych.¹⁶⁶

13.4. Pozostała część procedury przebiega bez incydentów, czynności urzędu imigracyjnego idą sprawnie, przy czym zabierają kilka minut dłużej w przypadku Yasmin i Geety przy odprawie ich pakistańskich paszportów, odbiór bagażu odbywa

¹⁶⁵ Po części ma rację. Jednakże rzeczywistym powodem ich zatrzymania jest to, że zostali oni poddani procedurze „profilowania pasażerów”. W tym przypadku pan Jones zarezerwował wakacje korzystając z opcji last minute, odbył w ostatnim czasie podróż do Pakistanu, dwie osoby należące do rodziny posiadające pakistańskie paszporty, a to, że poprosiły o osobne miejsca (wszystkie dzieci chciały siedzieć przy oknie) spowodowało, że zostali oznaczeni jako pasażerowie wysokiego ryzyka, w przypadku których zachodziła potrzeba przeprowadzenia dodatkowych kontroli. Profilowanie jest częścią próbnej procedury *Project Semaphore* wprowadzanej w ramach programu „e-granice” rządu Zjednoczonego Królestwa na wybranych lotniskach od 2004 r. Pierwotnie miał on obejmować sześć milionów pasażerów rocznie odbywających loty międzynarodowe kierujące się do Zjednoczonego Królestwa i upuszczające ten kraj. Program ten wykorzystuje technologię internetową i zaawansowane informacje dotyczące pasażerów dostarczone przez linie lotnicze policji celnej i pracownikom urzędu imigracyjnego przed przylotem w celu skontrolowania i odnotowania osób przylatujących i opuszczających Zjednoczone Królestwo, zapewniając w ten sposób rozbudowaną ścieżkę audytu przemieszczeń pasażerów, która może być stosowana w innych bazach danych. Zob. Home Office (2004) „Cutting-edge technology to secure UK borders [Najnowsza technologia w służbie ochrony granic Zjednoczonego Królestwa]”, 28 September, [http://press.homeoffice.gov.uk/press-releases/Cutting-Edge Technology To Secur?version=1](http://press.homeoffice.gov.uk/press-releases/Cutting-Edge%20Technology%20To%20Secure?version=1). W styczniu 2006 r. ogłoszono, że tego rodzaju działania mają objąć 40 milionów podróży krajowych odbywających się drogą lotniczą lub promem. Travis, A. (2006) „Security services and police to get UK air passenger details in advance [Służby bezpieczeństwa i policja mają otrzymywać z wyprzedzeniem dane dotyczące pasażerów samolotów w Zjednoczonym Królestwie]” *The Guardian* dnia 24 stycznia, <http://www.guardian.co.uk/airlines/story/0,1693586,00.html>.

¹⁶⁶ Po wydarzeniach z września z 2001 r. Stany Zjednoczone wprowadziły biometryczną identyfikację cudzoziemców przybywających do USA. Od 2004 r. w ramach programu USVISIT pasażerowie przybywający do Stanów Zjednoczonych i opuszczający je przechodzą kontrolę urzędnika ds. cel i ochrony granic Stanów Zjednoczonych, która obejmuje przegląd dokumentów podróży, takich jak wiza i paszport, pytania dotyczące pobytu w Stanach Zjednoczonych, a następnie pobranie odcisków palców wskazujących lewej i prawej ręki za pomocą bezatramentowego cyfrowego skanera. Ponadto urzędnik fotografuje twarz pasażera w formacie cyfrowym. Identyfikatory biometryczne są stosowane do potwierdzania tożsamości pasażera, dzięki czemu mogą być oni kontrolowani przy użyciu różnych baz danych w tym za pośrednictwem Systemu Informacji o Przylocie/Odlocie (Arrival Departure Information System (ADIS)), w którym przechowywane są informacje dotyczące przylotu i odlotu; Zaawansowanym Systemie Informacji o Pasażerach (Advance Passenger Information System (APIS)), który zawiera jawne informacje dotyczące przylotu i odlotu; Systemie Zarządzania Informacją z zastosowaniem Aplikacji Komputerowych 3 (Computer Linked Application Information Management System 3 (CLAIMS 3)), w którym przechowywane są informacje dotyczące cudzoziemców występujących o zasiłki; Międzyresortowym Systemie Kontroli Granicznej (Interagency Border Inspection System (IBIS)), który zawiera informacje obserwacyjne. IBIS ponadto jest połączony z bazami danych Krajowego Centrum Informacji Kryminalistycznej (Interpol and National Crime Information Center (NCIC)) databases; Zautomatyzowanego Systemu Identyfikacji Biometrycznej (Automated Biometric Identification System (IDENT)), który zawiera dane biometryczne cudzoziemców; Systemu Informacji o Studentach przebywających na Wymianie (Student Exchange Visitor Information System (SEVIS)), system zawierający informacje o studentach zagranicznych przebywających w TSanach Zjednoczonych; Ujednoliconej Konsularnej Bazy Danych (Consular Consolidated Database (CCD)), zawierającej informacje o tym, czy dana osoba posiada ważną wizę lub czy wcześniej ubiegała się o wizę. Zob. EPIC (2006) „United States Visitor and Immigrant Status Indicator Technology (US-VISIT) [Technologia określania statusu osoby przebywającej z wizytą lub imigranta w Stanach Zjednoczonych]”, <http://www.epic.org/privacy/us-us-visit/>. Zob. również: Department of Homeland Security (nd.) „US-VISIT Multilingual Videos and Brochures,” http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0435.xml.

się sprawnie.¹⁶⁷ Jednakże Ben i Toby ułożyli na wózku walizki jedna na drugą i w chwili gdy Ben skręca walizki spadają na Geetę, która zostaje przygnieciona. W chwili gdy Yasmin i Ben sprawdzają czy nic jej się nie stało, niemal natychmiast pojawiają się dwaj członkowie obsługi lotniska¹⁶⁸ i organizują elektryczny wózek dla pasażerów, który pomoże zabrać ich i ich bagaż do autobusu lotniskowego dowożącego pasażerów na parking.

14. Zakupy

14.1. Wyjeżdżając z lotniska, Yasmin włącza system Sat Nav, który wskaże im najkrótszą drogę do domu, ale również ostrzeże o obecności urządzeń do pomiaru prędkości i kamer rejestrujących pojazdy przejeżdżające na czerwonym świetle, jakie znajdują się na drodze. Yasmin wie, że nie potrzebuje, aby jej przypomniano o ograniczeniach prędkości, jednakże bez Sat Nav Gareth by o nich nie pamiętał. Dostał już sześć punktów karnych za przekroczenie prędkości, a kolejne sześć wiązałoby się z zakazem prowadzenia na rok, na co nie może sobie pozwolić biorąc pod uwagę jego codzienną drogę do pracy.¹⁶⁹

14.2. W drodze powrotnej planują zatrzymać się w wielkim, położonym poza miastem centrum handlowym. Gareth i Yasmin chcą iść do znajdującego się tam supermarketu, NSC, i kupić coś na kolację, podczas gdy dzieci idą do „Denim Warehouse”, gdzie jest wyprzedaż. Yasmin robi rodzinne tygodniowe zakupy spożywcze w poniedziałek po pracy. W Denim Warehouse Ben kupuje nowe dżinsy zachęcony darmową czapeczką baseballową, jaka była do nich dodawana, którą zakłada Tobiemu gdy opuszczają sklep. Sytuacja zmienia się gdy siedzą na ławce z Sarą, która spotkała kilkoro „Gotów”, kiedy zjawia się dwóch strażników nakazując Tobiemu zdjąć czapkę i prosząc ich, aby sobie poszli. Kiedy Ben zaczyna protestować, mówiąc, że nie mają do tego prawa, zostaje szorstko poinformowany, że jeśli sobie życzy może udać się do biura kierownika, gdzie dostanie kopię regulaminu centrum handlowego.¹⁷⁰ Wówczas za namową siostry przestaje się spierać i wszyscy udają się do samochodu.

14.3. Podczas gdy dzieci i Geeta są w samochodzie wraz z bagażem i prezentami, rodzice biorą mleko, chleb, sałatkę, pizzę i butelkę wina i kierują się do kasy. Planują zjeść tego wieczoru wspólny posiłek, po czym Yasmin odwiezie Geetę do jej mieszkania. Kiedy Gareth otwiera portfel okazuje się, że nie ma żadnej gotówki żeby zapłacić za zakupy, tylko kilka dolarów amerykańskich, które zostały mu z wakacji. Zazwyczaj korzystają z karty kredytowej wydanej przez NSC, ponieważ im

¹⁶⁷ Jest ono również usprawnione dzięki oznaczeniu bagażu kodem kreskowym, który pomaga liniom lotniczym rejestrować przemieszczenie i przeznaczenie bagażu w internetowej bazie danych.

¹⁶⁸ Zostali wezwani przez radio z centrali systemu monitoringu CCTV, który zarejestrował całe wydarzenie.

¹⁶⁹ Wyposażył samochód w najnowszej klasy detektor kamer Snooper S4 Evolution, który według sprzedawcy korzysta z najnowszej technologii GPS. Detektor może zlokalizować stacjonarne urządzenia pomiaru prędkości takie jak Gatsos, Truvelo, SPECS, mobile, DS2, Watchman i SpeedCurb. Jest on wyposażony w system głosowy i podaje nawet ograniczenie prędkości jakie występuje przy każdym zlokalizowanym urządzeniu do pomiaru prędkości. Przy ponad dwóch milionach osób, którym postawiono zarzuty na podstawie wydruków w automatycznych urządzeniach do pomiaru prędkości i kamer rejestrujących pojazdy przejeżdżające na czerwonym świetle, czujniki ostrzegające o tego rodzaju urządzeniach instalowane w samochodach stają się coraz bardziej popularne wśród osób, których praca wiąże się z prowadzeniem pojazdu. Szczegółowe informacje na ten temat są dostępne na stronie: [SpeedCameraDetectors.Com](http://www.speedcamerasuk.com/snooper-camera-detector.htm) (2006) ‘Snooper Speed Camera Detectors,’ <http://www.speedcamerasuk.com/snooper-camera-detector.htm>.

¹⁷⁰ Ochrona została zaalarmowana przez system monitoringu zainstalowany w sklepie i musi postępować zgodnie z surowymi wytycznymi w zakresie egzekwowania kodeksu klienta centrum handlowego. Stanowi on (miedzy innymi), że nie zezwala się na: „Wszelkiego rodzaju zastraszanie naszych Gości przez grupy osób lub pojedyncze osoby. Wszelkie grupy składające się z co najmniej pięciu osób, które nie zamierzają dokonać zakupu będą proszone o opuszczenie centrum”, „niespójne zachowanie wpływające negatywnie na środowisko centrum”, a także „noszenie wszelkich części ubioru ograniczających widoczność twarzy lub głowy (np. noszenie kaptura lub czapczek baseballowych) za wyjątkiem religijnych nakryć głowy” zob. np. Kodeks zachowania gości Bluewater Shopping Centre <http://www.bluewater.co.uk/home/guest-services/facilities/guest-conduct>.

częściej z niej korzysta, tym więcej dostaje kuponów bezgotówkowych i zwiększa w ten sposób swój limit kredytowy. Lubią korzystać z tego rodzaju kuponów, ponieważ są one związane z rzeczami, które kupili w przeszłości w NSC, a niekiedy używają ich w celu wypróbowania produktów, których by normalnie nie kupili, chyba że po niższej cenie.¹⁷¹ Gareth umieszcza kartę w czytniku i podaje swój PIN. Na zielono czarnym ekranie czytnika pojawia się komunikat nakazujący kasjerowi żądanie kolejnej autoryzacji karty. Patrząc z niedowierzaniem na ekran czytnika, Garteń czuje w kieszeni kurtki wibracje swojej komórki. Dzwoni zespół ds. przestępstw bankowych NSC! Oficjalny damski głos informuje go, że badają właśnie nietypowe transakcje dokonane jego kartą.¹⁷² Kobięcy głos pyta, czy jest świadomy tego, że jego karta była ostatnio używana na Florydzie, a teraz jest używana w Londynie? „Oczywiście” odpowiada. Podczas gdy Garteń informuje bank o odbytej podróży, Yasmin pośpiesznie podaje ich inną wspólną kartę kredytową, aby zapłacić za towary oraz kartę programu lojalnościowego.^{173 174} Jednakże po podaniu PINu karta zostaje odrzucona. Najwyraźniej na Florydzie wykorzystali nawet jej limit kredytowy, dziwne, że nie zdali sobie z tego sprawy. W tym czasie Gareth skończył rozmawiać przez telefon i może zapłacić za zakupy swoją odblokowaną kartą kredytową. Wracają do samochodu chwilę po tym, jak Geecie udało się udobruchać troje sprzecających się i zmęczonych długą podróżą dzieci i udają się do domu.

15. W domu

- 15.1. Ben i Toby rozpakowują bagaże, a Yasmin otwiera drzwi frontowe w ich domu w Finchley w północnym Londynie. Ich sąsiedzi, poproszeni o odbieranie ich poczty, najwyraźniej wyjechali na kilka dni i Yasmin musi siłować się ze starzejącymi się drzwiami z PCV, żeby z trudnością przecisnąć się do środka przez olbrzymią stertę listów i gazet leżących po drugiej stronie. „Od kiedy cieszymy się takim powodzeniem?” – myśli. Przy krzykach wchodzącej do środka rodziny zbiera pocztę i rzuca wszystko na stół kuchenny. Po rozpakowaniu bagażów Yasmin zaczyna przeglądać listy z filiżanką gorącej herbaty w ręku. Wyciąga zwykle rachunki za karty kredytowe, wyciągi bankowe, powiadomienia o podatku lokalnym i bezpłatne gazety lokalne. Znajduje też dwa listy dla Bena i trzy zaadresowane do niej i Garetha, które najwyraźniej przyszły ze szkół Toby’ego i Sary. Pozostałe papiery to druki bezadresowe¹⁷⁵, oferty ubezpieczeniowe i reklamy podwójnych szyb, próbki kosmetyczne, katalogi odzieży sportowej, a nawet przykuwająca wzrok reklamówka tanich lotów. „Ciut za późno”, potem rozbawia ją kolejna o produktach dla zwierząt, zaadresowana do ich ulubieńca, labradora, Dana Jonesa. Zakupili ostatnio dla niego ubezpieczenie dla zwierząt i najwidoczniej zapomnieli zaznaczyć pola „zrezygnuj” w liście adresowej.

¹⁷¹ Źródła danych dotyczących konsumentów zostały omówione w sekcji „Kluczowe elementy rozwoju” w raporcie eksperta ds. nadzoru konsumenta.

¹⁷² Nadużycia w zakresie danych dotyczących konsumenta zostały omówione w sekcji „Komentarz krytyczny i przyszłe wytyczne” w raporcie eksperta ds. nadzoru konsumentckiego.

¹⁷³ Programy lojalnościowe dla konsumentów zostały omówione w sekcji „Komentarz krytyczny i przyszłe wytyczne” w raporcie eksperta ds. nadzoru konsumentckiego.

¹⁷⁴ Karta programu lojalnościowego pozwala jej na gromadzenie punktów w określonej liczbie punktów sprzedaży, w tym w supermarketach NSC, Johnson Holidays, i w Wilsons, krajowej sieci agencji podróży. Poprzez zarezerwowanie wakacji za pośrednictwem Johnson Holidays, Yasmin zgromadziła wystarczająco dużo punktów, aby opłacić wycieczkę „city break”, której reklamę widziała w witrynie Wilsons. Chce zrobić Garethowi niespodziankę w rocznicę ślubu, która przypada w dalszej części roku. W popularnych programach lojalnościowych, takich jak Nectar card, punkty są zdobywane za każdego funta wydanego w uczestniczących w programie punktach sprzedaży. Na przykład jeden punkt Nectar jest równy 0,005p w Sainburys lub Argos i może być zrealizowany również w innych punktach sprzedaży. W celu uzyskania szczegółowych informacji zob.: <http://www.consumerdeals.co.uk/nectar.html>.

¹⁷⁵ Usługa *door to door* brytyjskiej Royal Mail umożliwia reklamodawcom uzyskanie obsługi równoczesnej na podstawie kodu pocztowego, a nie adresów indywidualnych, <http://www.springglobalmail.com/royalmail/en/d2d/d2d.htm>.

15.2. Otwiera trzy listy za szkół. Pierwszy to list ze szkoły Sary, zapraszający na zebranie rodziców z sprawie propozycji wprowadzenia losowych testów na obecność narkotyków dla uczniów. W liście wyjaśniano, że podczas niedawnych procesów w Kent w pewnej szkole zanotowano radykalny wzrost wyników egzaminacyjnych, a spośród 600 testów przeprowadzonych na uczniach w wieku 11-18 lat tylko jeden był pozytywny, co wskazuje na to, że program przynosi pożądany skutek. Jako że jest to kontrowersyjne posunięcie, szkoła chce jak najdokładniej je skonsultować przed podjęciem decyzji.¹⁷⁶ Drugi list, również ze szkoły Sary, opisywał szczegółowo nowy system kart dostępu, który zostanie wprowadzony w pierwszym tygodniu nowego semestru. System zostanie także wykorzystany do sprawdzania obecności i, jak pisało dalej w liście, z uwagi na kiepskie wyniki Sary w poprzednim roku szkoła wykorzysta system do zapewnienia rodzicom comiesięcznego sprawozdania z obecności¹⁷⁷ ich córki. W przypadku nieusprawiedliwionych nieobecności zostaną oni zaproszeni do szkoły w celu omówienia sprawy. Yasmin traci otuchę na myśl, że będą musieli porozmawiać o tym z Sarą. Jednak nastrój poprawia się, gdy czyta ona list z podstawówki Toby'ego: wygląda na to, że odtąd będzie dokładnie wiedziała, co każdego dnia Toby je na lunch. Szkoła wprowadza bezgotówkową kartę płatniczą na szkolne obiady. Jako część tego projektu rodzice będą mogli uzyskać dostęp do rejestru zakupów dziecka przez Internet. Yasmin zawsze podejrzewała, że Toby za pieniądze na lunch kupuje raczej chipsy niż owoce; teraz będzie mogła to sprawdzić!¹⁷⁸

15.3. Ben czmycha do swojej sypialni, żeby otworzyć listy. Pierwszy informuje go, że nie był karany sądownie i że dostał miejsce w projekcie VSO¹⁷⁹ i może spędzić sześć miesięcy pracując z ubogimi dziećmi w Afryce w ramach projektu zrównoważonego rozwoju.¹⁸⁰ Nie posiada się z radości, jednak drugi list sprowadza go z powrotem na ziemię. Jest to zapytanie, czy chce wziąć udział w konkursie kompletującym juniorską drużynę narodową Wielkiej Brytanii w badmintonie. Ben będzie musiał się nad tym zastanowić. Gra w drużynie szkolnej na poziomie hrabstwa, jednak wie, że jeśli ma wziąć udział w dowolnym konkursie ogólnokrajowym, jest dużo bardziej prawdopodobne, że będzie musiał zrobić losowy test na obecność narkotyków. W ciągu ostatnich kilku miesięcy zdarzało mu się palić trawkę w weekendy i dlatego boi się, że mogłoby to wyjść na jaw przy okazji testu.¹⁸¹

15.4. Po obiedzie Yasmin odwozi Geetę do jej pobliskiego mieszkania. Kiedy zmarł Deepak, mąż Geety, Geeta zamierzała przeprowadzić się do domu rodzinnego córki, ale było tam za mało miejsca. Zamiast tego rodzina postarała się o znajdujący się niedaleko dzienny dom opieki dla Geety. Robi się ciemno, gdy zajeżdżają na parking, ale Yasmin prawie tego nie zauważa, bo przy mocnym oświetleniu parkingu wydaje się być jasno jak w dzień. Nie dostrzega również kamer

¹⁷⁶ Blair, A. (2006) „Teenagers to face random drug testing at all schools [Nastolatki poddawane testom na obecność narkotyków we wszystkich szkołach]” *Times Online*, 31 maja, <http://www.timesonline.co.uk/article/0,,2-2204492,00.html>

¹⁷⁷ System pozwoli również na sporządzanie „pełnych raportów sądowych o zmianie miejsc uczniów, personelu i gości” i umożliwi „użytkownikom systemu stwierdzenie, kto wszedł gdzie i kiedy” g2is (nd.) „Access Controls Solutions for Schools [Rozwiązania kontroli dostępu w szkołach]” http://www.g2is.co.uk/pdfs/G235-G2_Access_Solutions_Schools.pdf.

¹⁷⁸ „Kontrola nawyków żywieniowych dzieci poza domem staje się ważną kwestią”, a przez Internet „bezgotówkowe rozwiązania g2 oferują rodzicom możliwość naniesienia wartości na kartę dziecka, monitorowanie i kształtowanie codziennych wydatków, przeglądanie, a nawet ograniczanie zakupów określonych rodzajów żywności” g2is (nd.) „Cashless Solutions for Schools [Rozwiązania bezgotówkowe dla szkół]” http://www.g2is.co.uk/pdfs/G231G2_Cashless_Solutions_Schools.pdf

¹⁷⁹ Voluntary Service Overseas.

¹⁸⁰ Zaświadczenie z rejestru sądowego jest obecnie obligatoryjne dla osób poszukujących zatrudnienia w zawodach wiążących się z opieką nad młodymi lub bezbronnymi. Zob. raport eksperta od przestępczości i wymiaru sprawiedliwości

¹⁸¹ Jako część „Narodowej polityki antydopingowej” brytyjskiego sportu, wszystkie narodowe stowarzyszenia sportowe muszą wdrożyć procedury losowych testów na obecność narkotyków. Testy powinno się przeprowadzać na wszystkich uczestnikach, biorących udział w konkursach zorganizowanych lub związanych z narodowymi stowarzyszeniami. W sezonie 2005/6 przeprowadzono około 7.968 testów w ramach 50 dyscyplin sportowych, z których 161 związanych z badmintonem, UK Sport (2006) „Drug free sport [Sport bez narkotyków]”, http://www.uksport.gov.uk/pages/drug_free_sport/.

monitorujących (CCTV), obejmujących wejście do bloku. Pozwalają one Terry'emu, tutejszemu dozorczy, mieć oko z zacisza jego biura na wchodzących i wychodzących. Gdy Geeta otwiera elektronicznym breloczkiem z kluczami automatyczne drzwi prowadzące do korytarza, Terry już czeka, by ich powitać i pomóc z bagażem.¹⁸²

- 15.5. Gdy Geeta zaczyna rozpakowywać swoje rzeczy, Yasmin sprawdza wszystko w mieszkaniu. Odkręca kurki, sprawdza elektryczność i gaz oraz czujnik ruchu w rogu. Jako że kilka miesięcy temu Geeta poślizgnęła się i straciła przytomność, rodzina poprosiła o zainstalowanie czujnika ruchu dla własnego spokoju.¹⁸³ Gdy tylko Geeta się ogarnęła, Yasmin wraca, żeby wcześniej położyć się spać, gdyż musi już następnego dnia iść do pracy.

16. Na mieście

- 16.1. Toby nie wraca jeszcze do szkoły przez jeden dzień, a Gareth bierze dodatkowy dzień wolny. To dzień pełen obowiązków; trzeba umyć samochód, kupić Toby'emu nowe buty do szkoły i telefon komórkowy, poza tym zaplanowali wizytę u matki Garetha, zabranie jej na lunch i zakupy. Matka Garetha mieszka po drugiej stronie Londynu, więc Gareth niechętnie uznaje, że szybciej będzie jechać przez centrum miasta.

- 16.2. Oznacza to przejazd przez strefę płatnego ruchu (Congestion Charging Zone), więc Gareth prosi Toby'ego, żeby przypomniał mu o zalogowaniu się na stronę Londyńskiego Transportu, gdy wróć do domu, żeby mógł uiścić opłatę przejazdową swoją kartą kredytową¹⁸⁴. System automatycznego rozpoznawania tablic rejestracyjnych (ANPR) czyta ich tablicę rejestracyjną 'GGJ 456', jednakże błoto na tablicy sprawia, że '5' rozpoznane jest jako '6' i dane samochodu są błędnie wczytane do bazy danych¹⁸⁵. Po opuszczeniu strefy płatnego ruchu Gareth zajeżdża na stację, żeby wreszcie umyć auto jak należy. Po drodze z garażu, przy wjeździe w ulicę jednokierunkową, Gareth nie uświadamia sobie, że inna, obsługiwana przez policję, kamera ANPR odczytała numer jego tablicy – tym razem prawidłowo. Gdyby o tym wiedział, zaniepokoiłoby go spostrzeżenie, że jego pojazd został zauważony przez zmotoryzowaną jednostkę policji drogowej sto metrów dalej. A to dlatego, że był uprzednio karany za jazdę pod wpływem alkoholu. Jednak jako że

¹⁸² Terry pracuje dla prywatnej agencji ochrony, a jego praca polega na śledzeniu monitorów telewizyjnych, słuchaniu rozmów i rejestrowaniu wydarzeń mających miejsce w miejscach publicznych bloku przy pomocy systemu audio oraz przyglądaniu się osobom wchodzącym do budynku i wychodzącym z niego. Gdyby nie widział kogoś przy wchodzeniu lub wychodzeniu przez dwa dni, ma za zadanie skontrolować daną osobę oraz powiadomić, w przypadku podejrzeń lub obaw, policję, służbę zdrowia lub opiekę społeczną. Zob. McGrail, B. (1999) *Highly Thought of? New Electronic Technologies and the Tower Block*, ESRC Virtual Society? Programme Research Report, Milton Keynes: The Open University.

¹⁸³ W lecie 2006 Rada hrabstwa Cheshire ujawniła „program telecare”, który finansuje instalacje sprzętu monitorującego w domach ludzi starszych, pomagającemu im w utrzymaniu niezależności. Częścią pakietu są windy schodowe, szyny, przyciski alarmowe, wykrywacze przelecia wody w zlewie i wannie, a także czujniki ruchu, które wykrywają czy osoba wstała z łóżka, czy przewróciła się. Czujnik ruchu jest w stanie wykryć formę ciała z dokładnością do 12 pikseli, zob. Cheshire CC (2006) „Alarms for elderly and disabled [Alarmy dla osób starszych i niepełnosprawnych]”, http://www.cheshire.gov.uk/socialcareandhealth/adults/alarms_for_elderly_and_disabled.htm.

¹⁸⁴ System opłat przekazowych korzysta z automatycznego systemu rozpoznawania tablic rejestracyjnych, który zapisuje w bazie danych numery rejestracyjne wszystkich samochodów, które wjeżdżają do strefy płatnej i ją opuszczają, jak napisano na stronie internetowej Transport for London (TfL): „Po przeczytaniu numeru rejestracyjnego pojazdu, porównuje się go z bazą danych pojazdów, na które wniesiono opłatę przejazdową na dany dzień. ... Po ostatecznym sprawdzeniu o północy (następnego dnia rozliczeniowego), komputer zatrzyma numery rejestracyjne pojazdów, których właściciele powinni zapłacić, jednak tego nie zrobili (włącznie z opłatami za poprzedni dzień rozliczeniowy). Sprawdzamy potem osobiście każde z zapisanych zdjęć przed wydaniem zawiadomienia o opłacie karnej.”, TfL (nd.) „Congestion Charging: imaging and cameras [Opłaty za korki – obrazy i kamery]”, <http://www.cclondon.com/imagingandcameras.shtml>.

¹⁸⁵ Konsekwencje tego są dla Garetha nieistotne: formalnie rzecz biorąc nie został zarejestrowany w systemie, więc nie będzie musiał uiścić opłaty, ale jako że tego nie wie, i tak ją zapłaci. Konsekwencje dla kierowcy samochodu o rejestracji GGJ 466, czy pani, która zabrała swoje auto na turystyczny wyjazd wakacyjny po Francji, zależeć będą o tego, czy osobiste sprawdzenie przed wysłaniem zawiadomienia o karze weźmie pod uwagę fakt, że są to dwa różne pojazdy – w rzeczywistości wyglądają bardzo podobnie.

wyrok ma już 4 lata, jest jedenasta przed południem, a samochód jest prowadzony w przyzwoity sposób, policjanci nie decydują się na zatrzymanie pojazdu¹⁸⁶.

- 16.3. Podczas gdy matka robi zakupy, Gareth z Tobym idą do „Mobiles4You”, żeby kupić nowy telefon. Toby już dawno marzył o komórce, większość jego kolegów już je ma. Myśli sobie, że byłoby odłotowo, gdyby przyszedł do szkoły z najnowszym modelem telefonu z wieloma fajnymi gram. Gareth jest właściwie zadowolony z tego, że Toby tak bardzo chce dostać telefon, bo odkąd sam chodzi do szkoły i z niej wraca, Yasmin chce mieć możliwość kontaktu z nim. Jednej rzeczy jednak Toby’emu nie powiedzieli – mianowicie, że zamierzają zarejestrować telefon w „Trace a Mobile.com”, co pozwoli im śledzić na bieżąco, gdzie przebywa ich syn – bez jego wiedzy¹⁸⁷.

17. Przestępczość a społeczeństwo

- 17.1. Yasmin odczuwa ulgę, że pierwszego dnia w pracy udało jej się uporać ze wszystkimi e-mailami i pilną pocztą do lunchu, a popołudnie może wykorzystać na przygotowanie do spotkania w sprawie projektu integracji młodzieży (Youth Inclusion Project, dalej YIP) w dalszym ciągu tygodnia. Jest tylko jedna pilna sprawa do załatwienia: Wilson Green, jeden z jej klientów, złamał zasady godziny policyjnej. Kilka miesięcy wcześniej Wilson został uznany za wielokrotnego recydywistę przez jej zespół do walki z przestępczością wśród nieletnich (Youth Offending Team) oraz w wyniku udanej operacji inwigilacyjnej wywiadu i policji został przyłapany na gorącym uczynku włamując się do miejscowej apteki¹⁸⁸. Mógł otrzymać karę pozbawienia wolności, jednak dano mu szansę udziału w intensywnym programie obserwacji i nadzoru (Intensive Surveillance and Supervision Programme, ISSP)¹⁸⁹. Jednakże zostali oni poinformowani przez Track-and-Track, prywatną firmę obsługującą system elektronicznego monitoringu, że w ciągu ostatnich dwóch tygodni trzykrotnie złamał narzuconą mu godzinę policyjną. W wyniku tego Yasmin będzie musiała wziąć udział w konferencji na jego temat, zaplanowanej na następny ranek, mającej na celu rozważenie, czy należy wysłać go z powrotem przed sąd z groźbą wtrącenia go do więzienia. „Jaka szkoda” – myśli.

- 17.2. Natomiast przydzielenie do YIP jest bardziej pozytywne. Podczas gdy większość prac w opiece społecznej skupia się na układaniu na nowo tego, co już się popsło, program YIP stara się zidentyfikować młodych ludzi najbardziej zagrożonych zostaniem przestępcami i udziela im wsparcia, gdy znajdują się w tarapatkach. W piątek odbędzie się spotkanie przeglądowe z udziałem wielu instytucji, mające na celu

¹⁸⁶ Kamera funkcjonuje jako część narodowego wspierania strategii ACPO (Association of Chief Police Officers) ANPR. Zob. raport eksperta od przestępczości i wymiaru sprawiedliwości.

¹⁸⁷ „Usługi lokalizacyjne służą do zlokalizowania telefonu innej osoby. Żeby usługa działała, telefon musi być włączony i musi znajdować się w zasięgu sieci. Usługi lokalizacyjne ukierunkowane do dzieci mają za zadanie uzupełniać normalny nadzór rodzicielski, a nie go zastępować. Dostarczają informacji o położeniu telefonu dziecka i w połączeniu z innymi formami komunikacji, takimi jak dzwonienie lub sprawdzanie, mogą pomóc rodzicom utrzymać kontakt z dzieckiem.” Trace a Mobile.com (2006) „Mobile phone tracking guide [Poradnik nt. śledzenia za pomocą telefonów komórkowych]”, <http://www.traceamobile.co.uk/mobiletrackingguide.php>.

¹⁸⁸ Dunnighan, C. i Norris, C. (1999) „The detective, the snout, and the Audit Commission: the real costs in using informants [Detektyw, kapuś i Komisja ds. Audytu – prawdziwe koszty wykorzystywania informatorów]”, *The Howard Journal*, 38(1): 67-86

¹⁸⁹ ISSP może kłaść nacisk na rutynowe testy na obecność narkotyków, żeby zapewnić, że przestępcy nie nadużywają zakazanych substancji, a także poddać przestępców wielu dodatkowym formom inwigilacji. Codziennie należy przeprowadzić co najmniej dwie kontrole z możliwością zwiększenia inwigilacji do nieustannego dwudziestoczęterogodzinnego monitoringu. Kontrole uwzględniają: monitoring osobisty kuratora sądowego prowadzony w określonym czasie w ciągu tygodnia i towarzyszący im w ustalonych zajęciach i spotkaniach, elektroniczny monitoring dla zapewnienia, że warunki godziny policyjnej są spełnione, weryfikacja sonogramu przez telefon dla zapewnienia, że dana osoba rzeczywiście przebywa tam, gdzie twierdzi, że przebywa; oraz jawna policyjna obserwacja kroków młodocianych przestępców w kluczowych momentach dla umocnienia programu, jak również dzielenia się informacją z personelem ISSP w Youth Offending Team (nd.) „ISSP: Surveillance [ISSP - nadzór]” <http://www.youth-justice-board.gov.uk/YouthJusticeBoard/Sentencing/IntensiveSupervisionAndSurveillanceProgramme/Surveillance.htm>.

ustalenie ostatecznej listy włączonych do programu. Program skupia się na miejscu, które Yasmin uważa za najgorszy teren komunalny w gminie to Dobcroft Estate. Jest to rozległe osiedle wysokościorców z lat sześćdziesiątych z ponad 2000 mieszkań i labiryntem betonowych pasażów. Yasmin wie, że większość dzieci na osiedlu skorzystałoby ze wsparcia, które mogłyby otrzymać, ale należy wybierać jedynie te najbardziej zagrożone przestępczością. Interwencje pociągają za sobą: zaangażowanie dzieci w lokalną działalność sportową, udział w zajęciach o uzależnieniu od narkotyków, zajęciach o radzeniu sobie z gniewem; przyprowadzenie ich matek i ojców na zajęcia poświęcone temu, jak być rodzicem; oraz – jej ulubione – nakłanianie dzieci do kręcenia filmów krótkometrażowych o problemach, z jakimi borykają się młodzi w tym rejonie. Zawsze jest zadziwiona, jak wiele zdają się zyskiwać dzięki takiemu doświadczeniu¹⁹⁰.

17.3. Przed wyjazdem na wakacje Yasmin poprosiła wszystkie agencje lokalne związane z dziećmi o wypełnienie formularza oceny ryzyka „dla ogółu młodzieży w wieku lat 13-17, zamieszkałej przy Dobcroft Estate, o której, dzięki waszej pracy lub za pośrednictwem ich rodzin, wiadomo wam, że jest zagrożona przestępczością”. Otrzymała już odpowiedzi z lokalnych szkół, policji, opieki społecznej, agencji Connexions, miejscowych kuratoriów oświaty (Local Education Authority) i komisji wymiaru sprawiedliwości dla nieletnich (Youth Justice Board). Ażeby mieć pewność, że nikogo nie pominięto, skontaktowała się również z miejscowym zrzeszeniem mieszkańców, zespołem pomocy potrzebującym ds. narkotyków i koordynatorem straży sąsiedzkiej (Neighbourhood Watch), żeby wysunęto kandydatury każdego dziecka, które przykuło ich uwagę. Każda z instytucji została poproszona o ocenienie zagrożenia dziecka przestępczością w skali 1-5 i dostarczenie istotnej informacji, która zostałaby użyta do ustalenia ogólnego stopnia ryzyka¹⁹¹.

17.4. Yasmin ma teraz za zadanie posegregować te wszystkie informacje w taki sposób, żeby można było skierować interwencję w stronę najbardziej zagrożonych. Uznaje, że najprostszym sposobem na początek jest posortowanie raportów według nazwisk – i stwierdzenie, czy jakieś dziecko nie zostało wymienione przez więcej niż jedną instytucję. Było wiele wielokrotnie wymienionych, ale jedno nazwisko się wyróżnia: trzynastoletni Darren White. Został zauważony przez sześć instytucji, znajdował się pod opieką władz lokalnych, ale obecnie znów mieszka z samotną matką, na jego starszym bracie ciąży seria wyroków, choć ma tylko 17 lat, regularnie wagaruje, zadaje się z podejrzaną grupą młodzieży i ma kontakt z narkotykami. Każde z wymienień jego nazwiska opatrzone oceną „4” lub „5”, wskazującą na wysokie ryzyko przyszłej przestępczości.

17.5. Do końca dnia zidentyfikowała 73 dzieci, które, po jej wstępnej ocenie, należy poddać dyskusji w piątkowym spotkaniu z udziałem wielu instytucji. Jutro powtórzy ten proces dla Junior Youth Inclusion Programme, mający na celu zidentyfikowanie jeszcze młodszych dzieci w niebezpieczeństwie: grupę wiekową 8-13.

17.6. Po drodze do domu Yasmin przegląda gazetę w autobusie i wzrok jej przykuwa nagłówek „Możemy podjąć zdecydowane kroki w sprawie społecznych dzieci

¹⁹⁰ Zob. część „Kluczowe elementy rozwoju” w raporcie eksperta ds. usług publicznych.

¹⁹¹ Formularz policyjny pyta na przykład, czy dziecko zostało aresztowane, skazane lub w inny sposób miało kontakt z policją w ciągu ostatnich sześciu miesięcy; formularz szkolny zawierał pytanie, czy dziecko zostało wyrzucone ze szkoły z ciągu ostatnich 12 miesięcy i czy regularnie opuszcza zajęcia. Formularz przeznaczony do wypełnienia przez koordynatora straży sąsiedzkiej zawierał pytania, czy dziecko sprawia kłopoty w danym terenie, czy należy do negatywnej grupy rówieśników, czy wiadomo o nim, że popełniło przestępstwo lub czy jego rodzeństwo lub inni członkowie rodziny mieli związek z popełnieniem przestępstwa, Youth Justice Board Youth Inclusion Programme (nd.) „YIP Core Group Referrals – Guidance For Partners [Kluczowe procedury policyjnego odesłania YIP – poradnik dla rodziców]” <http://www.youth-justice-board.gov.uk/NR/rdonlyres/0233E9E7-8E58-45E0-ACF8-E3190B8EAD19/0/ID50guidancedocumentforpartners.doc>.

jeszcze przed ich narodzinami” – mówi Blair.” Czytając artykuł zastanawia się, czy plan premiera, mający na celu interweniowanie w „trudnych rodzinach” przed narodzeniem dzieci, żeby nie wyrastały na chuliganów, nie był zbyt daleko posunięty. Jednak z drugiej strony – zastanawia się – być może jest to tylko logiczne rozwinięcie tego, co ona już teraz robi, być może jest to jedyny logiczny sposób wykorzystywania danych do przewidywania i kontroli zachowań¹⁹².

18. Biuro obsługi klienta

18.1. We wtorek rano Gareth wraca do pracy. Pracuje jako menedżer w dziale obsługi klienta w Sentasi Group, które jest właścicielem kilku biur obsługi klientów (multi-client call centres)¹⁹³. Wchodzi do budynku, wkładając do czytnika kartę RFID. W tym samym czasie system odnotowuje czas jego przybycia. Jego zdjęcie ukazuje się na ekranie w pomieszczeniu ochrony, która jest w stanie zlokalizować jego położenie, gdyż używa on karty przy wchodzeniu do różnych części budynku i ich opuszczaniu¹⁹⁴. Jego praca wiąże się z zarządzaniem dwoma dużymi projektami. Pierwszy wiąże się z akwizycją przez telefon; jego zespół dzwoni do abonentów indywidualnych, aby przepisali się do sieci telefonicznej Novacom, który jest jego zleceniodawcą. Drugi z towarzystwem ubezpieczeniowym, które promuje nowy produkt niszowy o nazwie Platinum, skierowany do starszych, pewniejszych kierowców¹⁹⁵. Klienci również dzwonią, żeby zmodyfikować swoje dane, zażądać odszkodowania i odwołać swoje decyzje¹⁹⁶. Gareth musi codziennie zdawać zleceniodawcom sprawozdanie z wydajności pracy, a co tydzień musi składać pisemne sprawozdanie w celu wyjaśnienia wszelkich wahań statystyk telefonicznych. Jego praca ma swoje zalety. Poza comiesięczną premią zależną od wydajności projektów ma ostatnio możliwość współpracować bliżej z Novacomem przy tworzeniu wyspecjalizowanego biura obsługi klienta w Hyderabadzie. Poznawanie swoich odpowiedników w spółce zleceniodawcy sprawia, że pisanie sprawozdań na podstawie statystyk staje się dla niego o wiele prostsze¹⁹⁷.

18.2. W celu nabrania rozpędu po wakacjach Gareth zaplanował wczesne spotkania z liderami zespołów obu projektów. Projekt z Novacomem funkcjonuje bez zarzutu. Gareth obserwuje, ile czasu każdy z operatorów poświęcił na poszczególne rozmowy i ile z tych rozmów zakończyło się sprzedażą, a comiesięczne sprawozdanie, które otrzymał, pokazuje, że mimo iż wyjechał na wakacje, wydajność nie uległa pogorszeniu. Pomijając nowych pracowników, którzy jeszcze uczą się fachu, większość członków zespołu przewyższa cele sprzedaży. Gareth przypisuje to dobremu nadzorowi i urzędzeniu miejsca pracy i zastanawia się, czy powinien zwiększyć cele wydajności¹⁹⁸. Zarekomenduje również w tym miesiącu lidera zespołu do premii.

¹⁹² Woolf, M., „Failures' targeted at birth [Zajęcie się 'klęskami' w chwili ich narodzin]”, *The Independent*, 16 lipca 2006, <http://news.independent.co.uk/uk/politics/article1180225.ece>.

¹⁹³ Biuro obsługi wielu klientów to takie, którego główna działalność polega na świadczeniu usług łączności z wieloma firmami jednocześnie.

¹⁹⁴ Zob. część „komentarz krytyczny” w raporcie o ekspercie od nadzoru miejsc pracy.

¹⁹⁵ Zob. „Kluczowe elementy rozwoju” w raporcie eksperta ds. nadzoru konsumenta.

¹⁹⁶ Dzwoniący umieszczani są w kolejkach o różnym czasie oczekiwania i są przydzielani do pracowników o różnym poziomie umiejętności. „Złoci klienci” są obsługiwani najszybciej i przez najbardziej doświadczonych przedstawicieli, włącznie z liderami zespołów. Ci klienci są ubezpieczeni przez Platinum od ponad pięciu lat i mają pełne pokrycie ubezpieczeniowe. „Srebrni klienci” otrzymali pełne ubezpieczenie 0-5 lat temu, a „Brązowi” to ci dzwoniący, którzy nabyli ubezpieczenie od odpowiedzialności cywilnej.

¹⁹⁷ W tej sytuacji zleceniodawca uznaje Garetha za odpowiedzialnego za wydajność projektu i to on znajduje się pod obserwacją. Jako osoba dostarczająca sprawozdania z wydajności zleceniodawcy (przez email), Gareth odpowiada za statystyki. Rozwinięcie się bardziej osobistej relacji ze zleceniodawcą pomoże zhumanizować tę odległą, wytworzoną technologicznie sytuację.

¹⁹⁸ W ten sposób pozwala on doświadczonym członkom zespołu ukształtować własny poziom sprzedaży, chociaż stara się on również przesłuchać losowo kilka wybranych rozmów dla sprawdzenia, że nie odbiegają one od wskazań firmowych. Zob. „Kluczowe elementy rozwoju” w raporcie eksperta ds. nadzoru miejsca pracy.

18.3. Po upojeniu się nowościami z Novacomu Gareth wraca na ziemię pod wpływem nowin z Platinum. Z powodu niedawnego braku telefonów niektórzy pracownicy surfowali po Internecie dla zabicia czasu. Firma pozwala na trochę surfowania w celach prywatnych, o ile pracownicy wylogują się na ten czas z systemu telefonicznego. A to dlatego, że system telefoniczny w każdym momencie zapamiętuje ich czynności. Co tydzień komputer podsumowuje wydajność projektu w oparciu o dane statystyczne wygenerowane przez skomputeryzowany system telefoniczny. To właśnie te statystyki Gareth ma przekazywać zleceniodawcy¹⁹⁹. Długie okresy braku aktywności nie są bynajmniej dobrą wiadomością dla zleceniodawcy. Dział informatyczny również skrupulatnie monitoruje strony, które odwiedzali pracownicy²⁰⁰. Poinformował, że pewien pracownik w godzinach pracy spędza czas na prywatnym blogu. Zamiast zablokować stronę, pod nieobecność Garetha dział informatyczny przeczytał posty pracownika i poinformował lidera zespołu o ich treści. Po spotkaniu Gareth usadawia się, żeby przedrzeć się przez zaległe emaila i odświeżyć swą wiedzę o przepisach dyscyplinarnych firmy.

19. Zdrowie

19.1. W środowy poranek Geeta ma dosyć, bo nie wolno jej zjeść śniadania – nawet kromki chleba czy filiżanki kawy. Na kalendarzu na drzwiach kuchennych napisano grubym czerwonym flamastrem, że dzisiaj o 16:30 ma badania kontrolne dla kobiet (Well Woman Check). Miesiąc temu otrzymała od lekarza pierwszego kontaktu list ze skierowaniem do miejscowej kliniki dla kobiet (Well Woman Clinic) dla pacjentek po pięćdziesiątce. W liście, napisanym po angielsku i przetłumaczonym na urdu, tłumaczono, że jako starszej kobiecie grozi jej choroba serca²⁰¹, udar mózgu, cukrzyca, niewydolność nerek lub wątroby, a także rak szyjki macicy lub rak piersi. Podkreślano, że wczesna diagnoza każdej z tych chorób zwiększała szansę na przeżycie oraz że jej zdrowie i dobre samopoczucie są ważne. Po lekturze Geeta czuje, że jej życie wisi na włosku, i zastanawia się, czemu niektóre z tych testów są konieczne²⁰². W liście doradzono nie jeść ani nie pić niczego poza wodą przez 12 godzin poprzedzających kontrolę, gdyż zamierzają pobrać próbki krwi i moczu. Sprawdzą również jej wzrost, wagę i wzrok. W liście wspomniano także, że pielęgniarka porozmawia z Geetą o jej trybie życia i sposobie odżywiania i może przedstawić zalecenia. Była również mowa o wizytach w szpitalu na kontrolnych badaniach piersi, jeśli będzie to konieczne.

19.2. Geeta czuje się zniechęcona, gdy przypomina sobie jak opiekowała się swoimi rodzicami z bardzo niewielką pomocą medyczną. Jest jednak zadowolona, że publiczna służba zdrowia tyle o niej wie i tak dobrze się nią opiekuje²⁰³. Jej oboje rodziców zmarło na zawał serca i ciągle martwi ją to, że i ona może mieć te same problemy. Nie miała wiele do czynienia z brytyjskim systemem zdrowotnym, jako że oboje dzieci urodziła w domu w Pakistanie i przez większą część życia cieszyła się dobrym zdrowiem.

¹⁹⁹ W biurach obsługi klienta pracownicy siedzą przy stanowiskach komputerowych, do których dołączona jest niewielka konsola zwana „wieżą”. Wieża ma kilka przycisków do przyciskania przez pracowników, które mają związek z poszczególnymi aspektami pracy. Przyciski związane są z różnymi kodami zadań, np. „nie gotowy na telefon” (Nie gotowy); „gotowy na telefon” (Gotowy); „odbieram telefon” (Telefon); „kończę rozmowę” (Kończę); „kody dodatkowe” (Zadania dodatkowe) – to ostatnie dotyczy zadań w rodzaju segregowania, odpowiadania na emaila i przerw. Zleceniodawca i kierownictwo biura obsługi klienta ustala limity czasowe na każdy z kodów zadań i czas personelu jest ściśle monitorowany i punktowany. Punktacja jest uśredniana z zależności od czasu i używana przy ocenie pracownika i wydajności.

²⁰⁰ Zob. „Wprowadzenie” w raporcie eksperta ds. nadzoru miejsca pracy.

²⁰¹ Brytyjscy Azjaci (wywodzący się z Pakistanu, Indii, Bangladeszu lub Sri Lanki) są narażeni na większe ryzyko zawału serca. Zob. *Patent UK* (nd.) ‘Preventing Cardiovascular Disease,’ <http://www.patient.co.uk/showdoc/23068754/>

²⁰² Zob. „Kluczowe elementy rozwoju” w raporcie eksperta ds. nadzoru medycznego.

²⁰³ Zob. część „Kluczowe elementy rozwoju” w raporcie eksperta ds. usług publicznych.

- 19.3. Poprosiła Yasmin, żeby z nią poszła, ta jednak nie mogła z powodu zobowiązań w pracy. Za to Sara zaofiarowała się towarzyszyć jej, bo akurat zdąży po szkole. Geeta jest naprawdę szczęśliwa, że jej nastoletnia wnuczka znajdzie czas. W czasie jazdy autobusem Geeta nic nie mówi o swoich zmartwieniach, a Sara odrywa ją od nich rozprawiając o funkcjonowaniu kamer monitorujących (CCTV), co zasugerował jej znak na autobusie mówiący, że „dla bezpieczeństwa i ochrony pasażerów autobus został wyposażony w kamery monitorujące CCTV”, a także o jej niedawnej przygodzie, kiedy to została wyproszona z miejscowego centrum handlowego, bo miała chęć zakwestionować prawo ochrony do zmuszenia jej z jej znajomymi „za zwykłe siedzenie na ławce”. Geeta sądzi, że za tą historią coś jeszcze się kryje, ale z porozumiewawczym uśmiechem i ku wielkiej uldze Sary zgadza się nic nie powiedzieć o tym Yasmin²⁰⁴.

20. Szkoła i po...

- 20.1. W środę korytarze w szkole Bena wypełniają się zagubionymi studentami szukającymi sal. Choć raz zostawił on sobie wystarczającą ilość czasu, żeby trafić na miejsce. Zaczyna lekcję w południe, zmierza więc do stołówki, żeby spotkać kogoś znajomego. Nikogo jednak jeszcze nie ma, więc, jako że w kafejce internetowej jest wolny komputer, zajmuje to miejsce - głównie po to, żeby z bezpiecznej odległości przyglądać się ludziom. Nie potrzebuje szkolnego loginu, żeby wejść do sieci, zatem jest to idealna okazja do sprawdzenia konta na hotmailu przed lekcją. W skrzynce odbiorczej znajduje się 120 wiadomości; nie zna prawie żadnego nazwiska nadawcy. Najwidoczniej wiele kobiet o prowokacyjnych imionach chciałoby zapewnić mu porządną rozrywkę, zapewni mu to ‘ziołowa vłagra’ (sic) i inne podejrzone leki na choroby, które trudno byłoby mu sobie wyobrazić, może także skorzystać z taniego poprawiania piersi lub zarobić miliony, jeśli tylko pomoże byłej żonie jakiegoś byłego nigeryjskiego ministra gabinetu. Zawahał się chwilę, po czy wszystko skasował. Inny email niby to pochodzi z banku i prosi go o potwierdzenie szczegółów logowania online. Ben nie jest aż tak naiwny; wie o wszystkich tego typu przekrętach, więc i ten kasuje. Zastanawia go jednak, czemu dostaje tyle śmieci na maila²⁰⁵.
- 20.2. W końcu dostrzega mail od swojego kolegi Aarona z którym przed rokiem zdawał egzaminy na A-levels (na koniec szkoły średniej). Tak jak Ben, Aaron jest zaangażowany w działania antykapitalistyczne. Wspólnie brali udział w akcjach Masy Krytycznej i Stop Wojnie od 16 roku życia, chociaż rodzice Ben o tym nie wiedzą. W wiadomości napisano, że w Londynie odbędzie się demonstracja antykapitalistyczna w przyszłą sobotę, jest organizowana w tajemnicy, a on musi przesłać SMS-em numer komórki, żeby poznać szczegóły dotyczące miejsca spotkania. Ben odpowiada od razu, że zobaczy się z Aaronem na najbliższej stacji metra w sobotę rano. Ma nadzieję, że do tego czasu uzbiera trochę pieniędzy. Po południu musi udać się do biura zasiłków, żeby sprawdzić, czy ma prawo do zasiłku, a nawet, choć niechętnie, rozważyć ofertę pracy w biurze obsługi klienta w niepełnym wymiarze, złożoną mu przez ojca.
- 20.3. Wiadomość z biura zasiłków jest dobra, ale Ben denerwuje się, bo nie chcieli dać mu jednoznacznej odpowiedzi. Powiedziano mu, że skoro uczy się do jednego egzaminu na A-level, teoretycznie ma prawo do zasiłku. Jednakże zanim podejmą decyzję musi on wypełnić kwestionariusz dla urzędnika orzekającego, który

²⁰⁴ O zasadach zakazu wstępu do centrów handlowych zob. McCahill, M. (2002) *The Surveillance Web [Sieć nadzoru]*, Cullompton, Devon: Willan.

²⁰⁵ Zob. „Komentarz krytyczny i przyszłe wytyczne” w raporcie eksperta ds. nadzoru konsumenta; Wall, D (2001) „Mapping out cybercrimes in a cyberspatial surveillant assemblage [Mapowanie cyberprzestępstw w zbiorze nadzoru cyberprzestrzennego]”. In Ball and Webster (2003) *op cit.* n.149.

zdecyduje, w nieokreślonym terminie, czy Ben rzeczywiście „szuka pracy”²⁰⁶. Ben sądzi, że mama może wiedzieć, jak jest naprawdę, ale podejrzewa, że powiedziała by tylko, że załatwienie tego zajęłoby wieki. Jego matka często wraca z pracy narzekając, że niemożliwością jest uzyskanie właściwej informacji od ludzi pracujących w innych dziedzinach opieki społecznej²⁰⁷.

20.4. W międzyczasie Ben potrzebuje pieniędzy na weekend, więc wraca do domu, dzwoni do banku i pyta o saldo, a – w razie konieczności – prosi o niewielki debet. Ben cieszy się, że postanowił zadzwonić do banku z telefonu rodziców, a nie ze swojej komórki opłacanej z góry, bo każą mu czekać dziesięć minut. Potem musi odpowiedzieć na cztery pytania kontrolne: podać datę urodzenia, numer komórki, zawód i kod pocztowy, zanim cokolwiek mu powiedzą. Na szczęście ma wystarczająco dużo pieniędzy. Przeczytawszy ogłoszenia o pracy w lokalnych gazetach, które przewinęły się przez otwór w drzwiach podczas ich nieobecności, kieruje się z powrotem do szkoły, żeby sprawdzić, co się dzieje w kompleksie sportowym.

21. Rodzina

21.1. W czwartek wczesnym rankiem Gareth zastanawia się nad spotkaniem, które zapowiada się na bardzo trudne i czuje się winny. Mimo że już prawie doszedł do siebie po zmianie strefy czasowej w czasie lotu, opuścił dom w złym nastroju. Irytuje go Ben; podejrzewa, że zadawał się z „niewłaściwymi ludźmi”, tak jak Sara, a może na dodatek bierze narkotyki. Ben dziwnie się ostatnio zachowuje – jest bardziej apatyczny niż zwykle – i Gareth martwi się nie tylko o przyszłość syna, ale również o to, jaki przykład daje młodszemu bratu. Tego rana wrzasnął na Bena, gdy ten nie chciał wstać z łóżka, a potem warknął na Yasmin, która właśnie robiła kazanie Sarze, żeby była gotowa do wyjścia do szkoły na czas. Żadne z nich nie chce oglądać kolejnego okropnego sprawozdania z obecności córki, teraz tworzonego za pomocą identyfikatorów RFID, których nie da się zakwestionować.

22. Znowu w biurze obsługi klienta

22.1. Jego myśli wkrótce kierują się do spotkania z pracownikiem podejrzanym o nadużywanie firmowego sprzętu komputerowego, a także z kierownikami działu zasobów ludzkich i działu informatycznego. Od odprawy z liderami zespołów we wtorek otrzymał niektóre dokumenty z działu informatyki, wyszczególniające działania pracownika w Internecie. Zastanawia się, jak to załatwić. Zatrudniona, Asabe, pisała cynicznego bloga o pracy w biurze obsługi klienta. Większą część bloga napisała w wolnym czasie na domowym komputerze, ale przy porównaniu informacji podanych przez informatyków z harmonogramem dyżurów zauważył, że pisała również w czasie pracy²⁰⁸. Z drugiej strony, gdy ponownie sprawdza statystyki wydajności Asabe z ostatnich kilku miesięcy, okazuje się, że jest ona najwyższej notowana. Odbiera odpowiednią liczbę telefonów, osiąga wysoką jakość, od razu rozwiązuje większość wątpliwości, a jej punktualność jest bez zarzutu. Trzyma się wyznaczonych przerw na lunch, herbatę i wyjścia do łazienki. Na papierze nie ma problemu²⁰⁹. Gareth odczuwa ulgę.

²⁰⁶ The Advice Centre (nd.), „Funding and benefits: Part-time students [Fundusze i dodatki – studenci studiujący w niepełnym wymiarze godzin]” <http://www.advice-centre.info/Part-Time%20Benefits.pdf#search=%22benefits%20for%20part%20time%20students%22>

²⁰⁷ Zob. „Kluczowe elementy rozwoju” w raporcie eksperta ds. usług publicznych.

²⁰⁸ Zob. „Komentarz krytyczny i przyszłe wytyczne” w raporcie eksperta ds. nadzoru miejsc pracy.

²⁰⁹ Zob. „Kluczowe elementy rozwoju”, *ibid.*

- 22.2. Na spotkaniu Asabe, która pochodzi z Nigerii, tłumaczy się. Blog zawiera zanonimizowane historie o jej spotkaniach z kierownikami i kolegami z biura obsługi klienta. Okazuje się, że Asabe czuje się prześladowana przez zazdrosnych kolegów z powodu jej wysokiej wydajności i uważa, że jest zastraszana. Niestety, jej kolor skóry stał się powodem prześladowań. Uważa ona, że liderzy jej zespołu przymknęli na to oko, mimo że informowała ich o swoich kłopotach. Jako że musi pracować, żeby zaoszczędzić na studia uniwersyteckie, zaczęła blogować o swoich przeżyciach, żeby poradzić sobie ze stresem. Niestety Asabe nieumyślnie ujawniła lokalizację swego miejsca pracy w blogu. Na spotkaniu dano wyraz problemom prawnym: firma została publicznie rozpoznana, a jej kierownictwo skrytykowane w sposób, który może doprowadzić do odpowiedzialności karnej zgodnie z ustawą o stosunkach rasowych (Race Relations Act), jeśli Asabe zdecyduje się pozwać ich do trybunału pracy. Istnieje niebezpieczeństwo, że jeden z najlepszych pracowników odejdzie. Co więcej, Asabe jest wściekła, bo szpiegował ją pracodawca. Wystąpiła sytuacja patowa²¹⁰.
- 22.3. Pod koniec spotkania dział zasobów ludzkich postanawia przeprowadzić dochodzenie z sprawie zarzutu o prześladowanie. Zachęcają Asabe, żeby prowadziła mniej publiczny zapis wypadków, w których była prześladowana i stale informowała lidera swojego zespołu, żeby można było zidentyfikować winnych. Jednakże Asabe czuje się podwójnie pokrzywdzona: była obiektem prześladowania, *jak również* inwigilacji. Twierdzi, że poszuka innej pracy i rozważy zasięgnięcie porady prawnej. Gareth żałuje, że go nie było i nie mógł pomóc liderowi zespołu na samym początku. Ma przeczucie, że całą sprawą należało pokierować na spokojnie, i że firma powinna była wesprzeć Asabe, a nie dochodzić własnego dobra prawnego²¹¹. Czekać na weekend ma nadzieję, że reszta tygodnia będzie spokojniejsza.

23. Oszustwo

- 23.1. Piątek na szczęście upływa spokojnie. Wszyscy wracają do Finchley wczesnym wieczorem, czeka ich odprężający weekend. Kiedy Gareth z Yasmin przygotowują obiad, Yasmin porusza temat rachunku za wspólną kartę kredytową, który przyszedł, gdy byli w pracy. Oboje wiedzą, że sporo wydali na wakacjach, ale Yasmin wyleciało z głowy, że karta została odrzucona wcześniej w tym tygodniu, więc oboje dziwią się wielce z powodu wysokości rachunku. Nie dość na tym; karta osiągnęła maksimum na transakcjach, których wcale sobie nie przypominają: na rachunku znalazły się zakupy w sklepach z odzieżą i restauracjach w Kalifornii, a przecież nie było ich w Kalifornii. Co gorsza, wygląda na to, że karty użyto do płacenia za dostęp do stron internetowych o nazwach brzmiących pornograficznie albo jeszcze gorzej. Yasmin jest przerażona. Czytała ostatnio o gwiazdzie pop, którą wpisano do rejestru osób, które dokonały przestępstw na tle seksualnym (Sex Offenders Register) za wchodzenie na takie strony z pornografią dziecięcą. Jeżeli ją śledzą, co pomyśli jej szef? Nawet jeśli jest niewinna, a przecież jest, ludzie zaczną gadać i rozniosą się plotki. Mogłaby nawet stracić pracę. Przez chwilę kusi ją, żeby sprawdzić na domowym pececie, co rzeczywiście zawierają te strony, ale uświadamia sobie, że to tylko dostarczy dowodów na to, że oglądała te strony, skoro zostanie to zapisane w czeluściach jej komputera.
- 23.2. Zamiast tego Gareth natychmiast dzwoni na numer serwisu klienta w sprawie rachunku. Wprowadza szczegółowe dane ich konta i po kilku sekundach zostaje przeniesiony do operatora z południowoafrykańskim akcentem. Wyjaśnia sytuację. Operator natychmiast zastrzega kartę i mówi, że w ich przypadku firma od kart

²¹⁰ Zob. „Kwestie nadzorujące”, *ibid.*

²¹¹ Zob. „Kluczowe elementy rozwoju”, *ibid.*

kredytowych zwróci stracone pieniądze na konto. Radzą również Garethowi, że powinien powiadomić większe firmy udzielające kredytów o zaistniałej sytuacji. Gareth wchodzi do sieci, prosi o odpis historii transakcji swojej karty kredytowej i o regularne aktualizacje w postaci emaili, żeby stwierdzić, czy jakieś nielegalne operacje kredytowe zostały poczynione w jego imieniu²¹².

- 23.3. Mocno udręczeni Yasmin, Gareth i dzieci jedzą wspólnie obiad. Wkrótce Sara znika na górze, żeby posłuchać ulubionej muzyki, Toby idzie grać po sieci na komputerze, a Ben mruczy coś o „ogarnięciu swoich spraw na jutro”. Yasmin i Gareth idą spać na kanapę, z której gapią się bezmyślnie na wiadomości i w końcu zasypiają.

24. Z powrotem na mieście

- 24.1. W sobotę rano Yasmin i Toby wychodzą na cotygodniowy basen. Kiedy idą do stacji metra, Yasmin dostrzega ogłoszenie straży sąsiedzkiej, które przypomina Yasmin, że musi odnowić swoją rejestrację. Na stacji muszą stać w kolejce, żeby kupić bilet Toby'emu. Było to denerwujące, bo Yasmin ma Oyster Card (kartę komunikacyjną), którą uważa za świetną, bo nie musi odtąd troszczyć się o odpowiednią ilość drobnych, żeby przejść przez bramkę metra. Przechodząc przez barierkę przesunęła tylko kartę nad czytnikiem, a opłata automatycznie obciążyła jej Oyster Card. Jako że zgodziła się na automatyczny kredyt wyrównawczy dokonywany przez sieć, na jej karcie nigdy nie brakuje pieniędzy, dopóki te są na jej koncie bankowym²¹³. Gdy czekają na peronie, Yasmin wie, że monitorują ich kamery rozległego systemu CCTV metra londyńskiego²¹⁴. Na basenie, mimo że wie, że strzegą ich ratownicy, nie uświadamia jednak sobie, że monitoruje ich również „Posejdon: trzecie oko ratownika”, który automatycznie wykrywa wszelkie przypadki możliwego utonięcia²¹⁵.

- 24.2. Ben również używa dziś swojej Oyster Card, jako że zgodnie z SMS-em, który otrzymał od organizatorów akcji „Stop Wojnie”, ma być w południe na stacji metra, na której jest zasięg sieci komórkowej, i mieć na sobie bejsbolówkę lub bluzę z kapturem, żeby kamerom monitorującym trudniej było zarejestrować jego twarz. Potem ma otrzymać SMS-a mówiącego o miejscu spotkania z innymi demonstrantami, a także, że ma się tam stawić w przeciągu 45 minut. Na stacji z łatwością dostrzega kumpla Aarona i organizatorów, którzy każą im iść pojedynczo lub dwójkami do placu Grosvenor i wchodząc z okolicznych ulic połączyć się przy Ambasadzie Amerykańskiej dokładnie o 13:30. Wtedy rozłożą wielki transparent z napisem „Stop Wojnie”, spróbują doręczyć ambasadorowi list protestacyjny, a rzecznik odczyta treść listu, stojąc przed transparentem. Całość zostanie sfilmowana i pokazana na żywo na ich stronie internetowej. Cała akcja ma potrwać poniżej dwóch minut, po czym wszyscy rozejdą się i każdy pójdzie w swoją stronę²¹⁶. Protest przebiega zgodnie z planem. W momencie, gdy policja dociera na miejsce,

²¹² Inside Out –East (2003) „Credit Card Cloning [Klonowanie kart kredytowych]” *BBC Online*, 7 lipca, http://www.bbc.co.uk/insideout/east/series3/credit_card_cloning.shtml

²¹³ Oyster Card to inteligentna karta korzysta z identyfikatora RFID do identyfikacji posiadacza i prowadzenia zapisu jego przejazdów. Jest to konieczne, ponieważ jeśli odbywasz kilka przejazdów tego samego dnia, w momencie gdy całkowity koszt tych przejazdów osiąga pewną określoną wartość, wszelkie następne przejazdy tego dnia odbędziesz za darmo, chyba że wyjedziesz poza strefę (strefy) objętą początkową wartością. TfL (nd.) *Oyster On-line*, <http://www.tfl.gov.uk/tfl/fares-tickets/oyster/general.asp>.

²¹⁴ Zob. McCahill and Norris (2003) *op cit.* n.44.

²¹⁵ „Posejdon” korzysta z komputerowego oprogramowania wizyjnego do identyfikacji przypadków utonięć, na przykład ciała, które pozostaje pod wodą przez dziesięć sekund albo więcej, Poseidon (nd.) „Technology overview [Przegląd technologiczny]”, <http://www.poseidon-tech.com/us/technology.html>.

²¹⁶ Wszystko to są środki antyinwigilacyjne. Protestujący są świadomi, że policja monitoruje ich stronę internetową, i podejrzewają, że ich telefony są na podsłuchu. Sądzą, że poprzez przekazywanie informacji w ostatniej chwili i używanie nowozakupionych komórek do wysyłania SMS-ów zmniejszają szansę przechwycenia informacji.

Ben i Aaron, odzyskawszy transparent, są już całkiem daleko i maszerują przez park św. Jakuba w drodze do stacji Waterloo, żeby spotkać się z kilkoma innymi demonstrantami i poznać najnowsze wieści o proteście. Po drodze mijają Parlament: w akcie brawury Aaron pospieszenie rozwija transparent i opiera go o wielkie czarne ogrodzenie, przekazuje Benowi komórkę i prosi go o zrobienie zdjęcia. Gdy Ben robi zbliżenie, czuje dotyk ręki na kołnierzu i głos mówi: „Jesteś aresztowany!”

24.3. Trzy godziny później zostają zwolnieni z aresztu policyjnego jedynie z nieformalnym ostrzeżeniem²¹⁷. Mimo że zostali przesłuchani, sfotografowani, pobrano ich odciski palców i pobrano ich DNA, odczuwają ulgę, że nie wyciągnięto względem nich dalszych konsekwencji²¹⁸.

24.4. Chłopcy nie wiedzieli jednak, że oficer, który ich zaaresztował, napisał raport wywiadowczy, który został godzinę później przejrany przez oficera prowadzącego dochodzenie w sprawie wcześniejszego „spontanicznego” protestu przed ambasadą. Zaintrygował go fakt, że podróżowali do stacji Marble Arch, i stąd podejrzewa, że tam właśnie było miejsce spotkania demonstrantów. Zastanawia się, czy mógłby uzyskać pozwolenie na udostępnienie mu bazy danych posiadaczy Oyster Card i dojść do nazwisk ludzi, którzy kończyli podróż na Marble Arch wcześniej tego dnia²¹⁹. Byłoby wspaniale, gdyby mógł zidentyfikować wszystkich demonstrantów, jednak z drugiej strony zbyt wielu byłoby do odsiania. Nie ma też pewności, czy dano by mu dostęp do tych danych, chronionych prawem, i pozwolono na takie całościowe ujawnienie²²⁰.

24.5. Ben tej nocy wraca do domu bardzo późno. Wcześniej wypił trochę z Aaronem, a teraz wślizguje się, kiedy wszyscy już poszli spać. Wróciła nawet Sara, która zaczęła przesiadywać ze znajomymi w pobliskiej budzie z hamburgerami aż do zamknięcia o 23:30. Ben wypija w kuchni półlitrową szklankę wody i cicho wchodzi po schodach, delikatnie zamyka drzwi sypialni i gasi światło.

25. Wniosek

25.1. Czy ten tydzień z życia rodziny Jonesów jest tak bardzo niezwykły? Duża część działań nadzorczych, z którymi mają do czynienia, a z których wiele jest zautomatyzowanych i niedostrzegalnych, dotyczy codziennie większości mieszkańców Wielkiej Brytanii.²²¹ Nadzór nad międzynarodowymi podróżami, mobilnością w przestrzeni miejskiej, wydatkami konsumenta, Internetem i mobilną telekomunikacją oraz nad potencjalną działalnością przestępczą stanowi obecnie element codzienności. Część z tych działań jest korzystna dla takiej rodziny i działania te są doceniane, ale też duża ich część wiąże się z osobistym zagrożeniem i ma znacznie szersze konsekwencje. Wykazaliśmy już, że nadzór ulega intensyfikacji

²¹⁷ Formalnie rzecz biorąc, złamali oni nowe prawo zabraniające organizowania protestów w odległości do jednego kilometra od Pałacu Westminsterskiego (Parlamentu) bez wcześniejszej zgody policji. Zob. „Parliament protesters fight ban [Protestujący spod Parlamentu walczą z zakazem]” *BBC News*, 31 sierpnia 2006, <http://news.bbc.co.uk/1/hi/england/london/5303558.stm>

²¹⁸ Obecnie policja może zdjąć odciski palców i pobrać próbki DNA od wszystkich aresztantów, nawet jeżeli nie zostali oskarżeni o popełnienie przestępstwa. Pozostaną one w państwowych bazach danych. Zob. Johnston, P (2003) „Police to keep DNA files of innocent [Policja przechowuje dane DNA osób niewinnych]” *Telegraph.co.uk*, 27 marca, <http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2003/03/27/ndna27.xml>.

²¹⁹ Przykład powstania nowej funkcji: po wprowadzeniu systemu Oyster Card jako prostej metody płacenia za transport publiczny, policja zdała sobie sprawę z tego, że dane z systemu mogą być przydatne przy śledztwach.

²²⁰ W 2004 roku policja londyńska (Metropolitan Police Service) tylko siedem razy zwracał się o informację przejazdów z Oyster Card, w 2005 roku liczba ta zwiększyła się do 243 życzeń, z których uznano 229. Zob. Jones, S (2006) „Oyster cards used to track criminals [Karty Oyster wykorzystuje się do śledzenia przestępców]”, *The Guardian*, 14 marca, <http://www.guardian.co.uk/crime/article/0,,1730518,00.html>.

²²¹ Zarówno Yasmin, jak i Gareth pracują w zawodach, w których występuje stosunkowo duża doza nadzoru, co pozwala nam na bardziej szczegółowe omówienie tej tematyki.

w wielu różnych sytuacjach: gdy dana osoba jest narażona na jakieś niebezpieczeństwo, gdy sytuacja prowadzi do przekroczenia reguł prawnych lub organizacyjnych, nawet we względnie uzasadnionych przypadkach. Najstarsi i najmłodszy członkowie rodziny odkrywają, że ich poruszanie się, otoczenie, i zawartość lub stan ich ciał są śledzone „dla ich własnego dobra i bezpieczeństwa”. Odbyna się to za pomocą mechanizmów i produktów, które są obecnie szeroko dostępne i reklamowane wśród mieszkańców Wielkiej Brytanii oraz dobrowolnie wybierane przez członków rodzin.

25.2. Nadzór nasila się, gdy członkowie rodziny są podejrzani o popełnienie przestępstwa, bądź też gdy padną jego ofiarami. Odchylenie (dewiacja) nabiera nowego znaczenia w prywatnych przestrzeniach w miejscu pracy, centrum handlowym i w szkole, gdzie właściwe dla danej organizacji przepisy określają, które zachowania są do przyjęcia, a które nie. Istnieją różne stopnie nasilenia nadzoru, które mają na celu albo rozwiązanie „trudnych” sytuacji, albo całkowite usunięcie ludzi. Konsumenci również potrafią łamać reguły: prowadzenie nadzoru nad konsumentami stawia wprawdzie w uprzywilejowanej sytuacji pewne osoby, ale jednocześnie stwarza sytuację niekorzystną dla innych. Taki stan rzeczy ilustruje opisany przypadek, dotyczący kart kredytowych, kart lojalnościowych i przesyłek masowych, napływających z profili konsumenckich Yasmin i Garetha, które umożliwiają im zakupienie różnych produktów po obniżonej cenie, podczas gdy Ben, klient o niskim statusie, zmuszony jest oczekiwać na linii na połączenie ze swoim bankiem na własny koszt. W przypadkach, w których mają miejsce nietypowe działania, wychodzi na jaw fakt, że bank cały czas ma oko na klienta. We wszystkich przypadkach, jakiegokolwiek nietypowe lub nieprzewidziane działania w odniesieniu do kategorii danej osoby wpływają na nasilenie nadzoru, czego następstwa mogą być różne.

25.3. Co jest ważne w odniesieniu do takiego splotu okoliczności? Oprócz tego, że stanowią one odzwierciedlenie naszych codziennych doświadczeń, to w ich świetle rysuje się wyraźniej wiele kwestii, których dotyczy niniejszy raport, a w szczególności przyczyny, skutki i doświadczenia wiążące się z nadzorem. Rodzina styka się z bardzo wieloma rodzajami nadzoru. Część z nich ma charakter jawny i otwarty, a część – skryty i drugoplanowy. Pełna lista przypadków, w których stykamy się z nadzorem, została przedstawiona w załączeniu. W niektórych przypadkach jedni ludzie decydują się na czynny udział w nadzorze, a inni – nie. Członkowie rodziny, skoro tylko znajdują się poza domem jako obywatele, konsumenci, podróżnicy i pracownicy, mają niewielki wybór co do tego, czy mają się stać przedmiotem nadzoru. W przypadku towarów konsumpcyjnych, a także nadzoru prowadzonego w portach lotniczych i w miastach przez policję i CCTV, rodzina jest nieświadoma tego, że nadzór stanowi zwykły element infrastruktury, ani też tego, jak wiele informacji na jej temat znajduje się w posiadaniu innych. W przypadku badań i nadzoru zdrowotnego w szkołach, odbiorcom doradza się, aby zgłaszali się do udziału „dla ich własnego dobra”, co jednak budzi zastrzeżenia, jeśli chodzi o rodzaj dokonywanych wyborów. Każda znacząca debata w sprawie społeczeństwa nadzorowanego będzie opierać się na tym, że obywatele przynajmniej w pewnym stopniu są świadomi tego, jakie informacje zostały zebrane na ich temat, gdzie zostały skierowane, co dzieje się z tymi informacjami i dlaczego. Debata taka dotyczyć będzie również tego, co można zrobić, aby uregulować nadmierny nadzór i tego, kto ma tego dokonać.

25.4. Pomimo takiego zróżnicowania, opisane przez nas procedury nadzoru mają jedną wspólną cechę: wszystkie one mają wpływ na szanse życiowe rodziny, podejmowanie decyzji i wzajemne stosunki. Uprzywilejowani konsumenci, tacy jak

Gareth, mają szybszy dostęp do usług niż jego „uboższy” syn – student, Ben. Domy i ciała ludzi podatnych na zagrożenia, takich jak Geeta i Toby, podlegają monitoringowi. W trakcie tego procesu tracą oni swoją autonomię i prywatność. Nawet bycie uznanym za osobę w niewielkim stopniu podejrzaną ma wpływ na zmianę zachowania. Yasmin jest świadoma, że odbywa się kontrola jej kartoteki kryminalnej, a Sara nie odpowiada pracownikom ochrony. Perspektywa zostania wykluczonym lub możliwość zmiany warunków porozumienia dotyczącego czyjegoś udziału w życiu społeczeństwa jawi się jako surowa konsekwencja i przemawia do najgłębszych obaw rodziny. Stąd też nie zaskakuje fakt, że rodzina wykazuje się ambiwalentnym stosunkiem do takiej perspektywy. Yasmin i Gareth używają w różnych miejscach uprawnionych technik nadzoru - aby chronić swoją własną zdolność kredytową, monitorują zdrowie i warunki życia swoich dzieci i matki Yasmin. W pracy korzystają oni z własnych sieci społecznych i stosunków, aby prowadzić mediację i interpretować dane uzyskane drogą nadzoru. W szczególności, wprowadzenie nadzoru do szkół, do których uczęszczają dzieci, uwypukla panujące w rodzinie stosunki i przyczynia się do nasilenia panujących napięć. Różnorodność doświadczeń związanych z nadzorem sprawowanym nad rodziną i mającym miejsce wewnątrz rodziny dowodzi, że podejście do „społeczeństwa nadzorowanego”, jako zjawiska jednorodnego, jest niewłaściwe. Jest to zjawisko dynamiczne, wielopoziomowe i złożone. Powstaje więc pytanie: co zdarzy się potem?

Część C/2

Obrazy z życia w społeczeństwie nadzorowanym, rok 2016

26. Wstęp

- 26.1. Duński fizyk Niels Bohr jest autorem znanego powiedzenia, że „przewidywanie jest bardzo trudną rzeczą, zwłaszcza jeśli dotyczy przyszłości”. Naszym zamiarem w tym miejscu nie jest wgłębianie się w dziedzinę futurologii czy przepowiadania. Uważamy jednak, że użyteczne byłoby przedstawienie tutaj kilku szkiców, które wykorzystywałyby pewne wydarzenia ze scenariusza i umiejscawiały je w niedalekiej przyszłości. Pragniemy w ten sposób zwrócić uwagę na pewne zmiany, jakie muszą wprowadzić ustawodawcy. Używamy takiego samego zestawu osób, jak w scenariuszu dotyczącym roku 2006, na takim samym etapie życia i cieszących się taką samą pozycją społeczną.
- 26.2. Proponując tematykę ogólną zakładamy, że przyszłe społeczeństwo nadzorowane będzie społeczeństwem nadzoru wszechobecnego, ukierunkowanego przede wszystkim na śledzenie i kontrolę wszelkiego rodzaju ruchomości (ludzi, przedmiotów i danych) oraz prognozowanie zachowań i zapobieganie im. Zakładamy też, że w dalszym ciągu będzie trwało przechodzenie władzy i uprawnień z rąk publicznych w prywatne.
- 26.3. Obrazy te nie powinny być odbierane jako oznaczające, że w praktyce wszystkie przedstawione systemy i procedury „zadziałają” dokładnie tak; zgodnie z tym, co przedstawiono w sekcji 9.11 powyżej, technologie mają swoje ograniczenia, a plany mogą nie powieść się. Jednakże dla celów, w jakich przedstawiamy nasze obrazy, przyjęliśmy założenie, że wszystko działa zgodnie z zapowiedzią.
- 26.4. Sceny te mają jednak dość zachowawczy charakter. Przedstawiona tu przyszłość w żadnym razie nie jest tak okrutna i autorytarna, jaka mogłaby być w istocie: założyliśmy, że panuje to samo połączenie opieki i kontroli, z jakim mamy do czynienia w Wielkiej Brytanii od czasów drugiej wojny światowej. Nie uwzględniliśmy możliwości wystąpienia nowych, gwałtownych wydarzeń – czyli katastrofy ekologicznej, wojny światowej lub domowej – które mogą zmienić charakter kategorii ryzyka z ustalonych scenariuszy w linie podziału wiążące się z brutalnymi konfliktami lub warunkami sprzyjającymi ludobójstwu. Nie należy w związku z tym uważać, że takie wydarzenia nie są możliwe: dochodziło do nich w przeszłości, dochodzi obecnie w innych częściach świata i może dojść ponownie gdziekolwiek.
- 26.5. Poniżej przedstawiamy 14 szkiców, zatytułowanych:
- Kontrola tożsamości
 - Przejścia graniczne
 - Zarządzanie zestawem otaczających nas marek (krajobrazem marek)
 - Bezgotówkowe zakupy
 - Mieć dzieci na oku

- Totalne rozwiązania społeczne?
- Zmiana zasad jazdy
- Przyjazne, latające oczy na niebie
- Niezidentyfikowana pod-klasa
- Wirtualne śledzenie
- Twoje życie to nasza sprawa
- Troska o ciebie
- Lustrzany korytarz

27. Kontrola tożsamości

27.1. Wracając z Florydy do Wielkiej Brytanii w 2016 roku, rodzina Jonesów styka się z dość odmienną scenerią, niż rodzina z roku 2006. Na podstawie tego, czego doświadczają oni na granicy, trudno jest dostrzec różnicę między dwoma krajami. Usługi związane z imigracją i kontrolą graniczną zostały zlecone, zarówno przez Wielką Brytanię, jak i Stany Zjednoczone oraz wszystkie państwa Unii Europejskiej i wysoko uprzemysłowione państwa grupy G10, temu samemu ponadnarodowemu prywatnemu konsorcjum BorderGuard (Straż Graniczna).²²² Ciągła obawa przed nielegalną imigracją i rządowa retoryka „wojny z terroryzmem” doprowadziły do tego, że rządy tych państw zamówiły i wdrożyły mechanizm „inteligentnej granicy”, oparty zarówno na technologiach nadzoru jawnego, jak i niejawnego.

27.2. Kontrola paszportów odbywa się teraz przy pomocy zestawu kamer i czytników, które rejestrują obrazy twarzy, tęczy i palców, które następnie porównywane są z danymi zapisanymi w znormalizowanych paszportach biometrycznych lub, w przypadku Wielkiej Brytanii, kartach identyfikacyjnych, wprowadzonych w państwach G10 i Unii Europejskiej.²²³ Paszport lub karta identyfikacyjna jest również odczytywana przez odpowiednie urządzenie. Liczne dane, zapisane na wbudowanym w kartę chipie RFID obejmują teraz wszystkie informacje dotyczące obywatelstwa, imigracji, wiz i karalności, a także informacje dotyczące zdrowia. Są one natychmiast porównywane z państwowymi i ponadnarodowymi bazami danych, podobnie, jak cała gama pozyskiwanych danych dotyczących transakcji konsumpcyjnych, jaką BorderGuard otrzymuje regularnie od specjalistycznych firm.²²⁴

28. Przejścia graniczne

²²² Patrz: Borders Expert Report [Specjalistyczny raport w sprawie granic].

²²³ Międzynarodowy Urząd Lotnictwa Cywilnego (International Civil Aviation Authority – ICAA) uzgodnił standardy dotyczące dokumentów podróży o odczycie maszynowym (Machine Readable Travel Documents – MRTD) w 2004 roku. Proces ten kierowany był przez Inicjatywę na rzecz Zwiększenia Bezpieczeństwa i Ułatwienia Podróży Międzynarodowych (Secure and Facilitated International Travel Initiative - SAFTI) w obecnej grupie G-8, patrz: *Statewatch* (2004) „G8 meeting at Sea Island in Georgia, USA - sets new security objectives for travel [Spotkanie grupy G-8 w State Island w stanie Georgia, USA – ustanowienie nowych celów w zakresie bezpieczeństwa podróży]”, <http://www.statewatch.org/news/2004/jun/09g8-bio-docs.htm>. Doszło do tego pomimo obaw dotyczących łatwości kopiowania czipów RFID: Johnson, B. (2006) „Hackers crack new biometric passports [Hakerzy włamują się do nowych biometrycznych paszportów]”, *The Guardian*, 7 August (7 sierpnia) <http://politics.guardian.co.uk/homeaffairs/story/0,,1838754,00.html>. Fakt, że brytyjskie karty identyfikacyjne mogą łatwo zostać przekształcone w paszporty biometryczne lub połączyć się z nimi, już został dostrzeżony Lettice, J. (2005) „UK biometric ID card morphs into £30 ‘passport lite’ [Brytyjskie biometryczne karty identyfikacyjne przekształcają się w wersję paszportu *light* za 30 funtów]”, *The Register*, 8 July (8 czerwca), http://www.theregister.co.uk/2005/07/08/id_card_as_passport/.

²²⁴ Patrz: Consumer Expert Report. [Specjalistyczny raport w sprawie konsumentów] W 2016 roku w dalszym ciągu trwają spory pomiędzy państwami i pracującą w charakterze zleceniobiorcy służbą graniczną, dotyczące kwestii własności intelektualnej danych dotyczących podróży. Rząd brytyjski zachowuje swoje prawo do „sprzedaży” danych dotyczących tożsamości, zgodnie z projektem wysuniętym w 2006 roku. Elliot, F., „ID plans: powers set to widen [Plany dotyczące dokumentów tożsamości: uprawnienia stają się coraz szersze]”, *The Independent*, 6 August (6 sierpnia) 2006, <http://news.independent.co.uk/uk/politics/article1216000.ece>. Jedyny głos, który jest głosem przegranym w tej sprawie, to głos obywatela.

- 28.1. Skutek wprowadzenia inteligentnych granic jest taki, że odprawa niektórych osób przebiega szybciej, a innych wolniej, w zależności od tego, czy ich kraj pochodzenia bierze udział w tym mechanizmie. Jednakże firma BorderGuard poczyniła pewne ustępstwa. Zezwoliła ona na szybszą odprawę obywateli państw nieuczestniczących w mechanizmie, pod warunkiem, że będą oni posiadać paszporty biometryczne. Pakistan wprowadzie nie uczestniczy w mechanizmie, ale daje swoim obywatelom możliwość wyrobienia paszportu biometrycznego, co jednakże wiąże się z poważnymi kosztami, które dana osoba musi ponieść sama.²²⁵ Geeta nigdy nie kupiła sobie paszportu biometrycznego i w związku z tym musi czekać kilka godzin, podlega różnego rodzaju dodatkowym przeszukaniom, a także musi odpowiadać na różne pytania.
- 28.2. Sara świadomie wybrała sobie szokującą powierzchowność modnej nastolatki. Mimo to w stosunku do niej nie ma żadnych podejrzeń, ale wyraźnie „azjatyckie” cechy Yasmin wywołują alarm. Gdy urządzenie skanujące jej kartę identyfikacyjną porównuje jej dane z utrwalonymi na obszarze USA zapisami dotyczącymi jej karty kredytowej, zostaje ona wezwana na przesłuchanie.²²⁶ Nie musi ona czekać na kolejne zakupy, aby dowiedzieć się, w jakim celu została wykorzystana jej podrobiona karta. Wymaga się od niej jednakże wyjaśnień dotyczących całego szeregu wątpliwych zakupów dokonanych na terenie kraju, którego nigdy nie odwiedzała. Zostaje zwolniona godzinę lub dwie później, po sprawdzeniu danych z zapisami z Florydy i ustaleniu, że jej karta została podrobiona.²²⁷ Mimo to bank nie zwróci pieniędzy na jej konto jeszcze przez kilka tygodni – niektóre rzeczy nigdy się nie zmieniają!
- 28.3. Przy odprawie celnej każda osoba zostaje poddana pełnemu przeszukaniu - wirtualnej rewizji osobistej z wykorzystaniem skanera pracującego na fali o długości milimetra.²²⁸ Sarze wydaje się, że słyszy sprośną uwagę celników na temat jej tatuażu²²⁹, ale nie ma sensu protestować, ponieważ może to tylko skupić na niej ich uwagę i wiązać się z dalszymi kłopotami.²³⁰ W każdym razie, jest całkiem możliwe, że wszystko, co powiedział urzędnik, zostało zarejestrowane przez mikrofony CCTV, używane do monitorowania pracy, i że to jego czekają problemy.²³¹

29. Zarządzanie zestawem otaczających nas marek (krajobrazami marek)

²²⁵ Rozważano już takie potencjalne problemy patrz np.: Koslowski, R. (2004) „International Cooperation to Create Smart Borders [Międzynarodowa współpraca nad stworzeniem inteligentnych granic]”, dokument przedstawiony w: *North American Integration: Migration, Trade, Security*, Ottawa, April 1-2 (1-2 kwietnia).
<http://www.irpp.org/events/archive/apr04/koslowski.pdf>

²²⁶ Nieformalne zaszeregowanie osób ze względu na rasę ma miejsce już obecnie i funkcjonuje już od dłuższego czasu. Takie postępowanie sugeruje również policja brytyjska, jako część formalnej polityki <http://www.timesonline.co.uk/article/0,,22989-1717624,00.html> Aby uzyskać więcej informacji zob.: <http://www.aclu.org/racialjustice/racialprofiling/index.html>

²²⁷ Połączenie baz danych może wiązać się z pewnymi skutkami pozytywnymi – zamiast niedogodności i prawdopodobnie jeszcze poważniejszych następstw sklonowania karty kredytowej, takich jak wielotygodniowe dochodzenia, pojawi się możliwość znacznie szybszego wykrycia i rozwikłania takich przestępstw, jak wskazuje na to przytoczony przykład.

²²⁸ Takie skanery przeszukujące całe ciało są już w stadium prób pilotowych. Istnieje kilka konstrukcji, na przykład operujący na promieniach rentgenowskich o niskim natężeniu aparat Secure 1000 firmy Rapiscan: <http://www.rapiscansystems.com/sec1000.html>, testowany na lotnisku Heathrow, patrz: Lettice, J. (2004) „See through clothes' scanner gets outing at Heathrow [Na Heathrow pojawił się skaner, który widzi przez ubranie]”, *The Register*, 8 November (8 listopada), http://www.theregister.co.uk/2004/11/08/heathrow_scanner_pilot/; działające na fali o długości milimetra skanery, nad którymi pracuje firma QinetiQ, wypróbowywane w Eurotunelu: http://www.qineti.com/home/newsroom/news_releases_homepage/2004/3rd_quarter/Next_generation_security_screening.html.

²²⁹ Badania przeprowadzone w pokojach kontrolnych CCTV latach 90-tych wykazały, że operatorzy używali sprzętu do wszelkiego rodzaju zachowań seksistowskich - technologia umożliwiająca uzyskiwanie tak intymnych obrazów może powodować podobne problemy. McCahill, M. i Norris, C. (1999) „Watching the workers: Crime, CCTV and the workplace [Nadzorowanie pracowników: przestępczość, CCTV i miejsce pracy]” w: Davis, P., Francis, P. and Jupp, V. (wyd.) *Invisible Crimes: Their Victims and their Regulation* [Niewidoczne przestępstwa: ich ofiary i przepisy]. London: Macmillan.

²³⁰ „Normalizacja” w pracy lub „efekt schładzający” społeczeństwa nadzoru.

²³¹ Z drugiej strony, dzięki nadzorowi możliwa jest ochrona przed molestowaniem lub ułatwione dochodzenie zadośćuczynienia.

- 29.1. Gdy rodzina Jonesów odwiedza miejscowe centrum handlowe, CCTV i ochrona cały czas funkcjonują, a kierownicy centrum wciąż dysponują siecią kontaktów, dzięki którym mogą zlokalizować niepożądane osoby i odseparować je od sklepów i kupujących. Jednakże modelowanie przestrzenne krajobrazu marek (brandscape)²³² i zmiana metod reklamy zgodnie z przepływem różnych kategorii konsumentów stanowi już priorytet strategiczny większości sprzedawców detalicznych. Pomiędzy właścicielami centrów handlowych a najemcami, czyli wielkimi sieciami handlu detalicznego rozwinęły się już nowe związki biznesowe.
- 29.2. Sieci handlu detalicznego umożliwiają centrum handlowemu dostęp do wielkiej, wspólnej bazy danych, tworzonej na podstawie danych z karty nagród, w celu uzyskania informacji dotyczących przepływu kupujących. System ten opiera się na wszytych w odzież identyfikatorach wykorzystujących technologię RFID, wszechobecnych czytnikach i zbiorach danych konsumenta. Czytniki umieszczone w drzwiach sklepów uczestniczących w systemie rejestrują niepowtarzalne kody identyfikacyjne zapisane we wszytych w odzież kupujących identyfikatorach. Informacje dotyczące danej sztuki odzieży, jej marki, miejsca zakupu oraz tego, kto ją kupił, porównywane są z profilami konsumentek różnych osób noszących odzież. Inteligentne ekrany umieszczone na wysokości oczu pokazują w czasie rzeczywistym reklamy wybranej gamy produktów odpowiadających temu konsumentowi. Sara zachwyca się widząc na ekranie reklamującym najbliższy sklep muzyczny nową obwolutę albumu jej ulubionego zespołu, a Toby zwraca uwagę na informację dotyczącą gier komputerowych. Do Bena niezupełnie to przemawia. Jak dotąd nic z tego, co zobaczył, nie zainteresowało go. Informacje marketingowe mogą również być przesyłane konsumentom do ich indywidualnych, podręcznych urządzeń, gdy znajdą się oni w sąsiedztwie pewnych sklepów.

30. Bezgotówkowe zakupy

- 30.1. Centrum handlowe pozyskuje następnie dane, aby „wyłować” tych klientów, którzy najczęściej korzystają z centrum handlowego, aby zaproponować im członkostwo w systemie zakupów „bezgotówkowych”. System ten umożliwia co „cenniejszym” konsumentom²³³ otrzymanie wszczepianego pod skórę chipa, który ułatwi im zakupy.²³⁴ Za implant płaci się 200 funtów. Następnie konsumenci mogą załadować na chip pieniądze i płacić w różnych sklepach zbliżając swoje ramię do czytnika, zamiast używać karty kredytowej, debetowej lub sklepowej. Reklamy systemu bezgotówkowego mówią kupującym, że jako posiadacze chipa uprawnieni są oni do otrzymania rabatu w wybranych przez nich sklepach w centrum handlowym,²³⁵ dzięki czemu poniesione przez nich na początku koszty implantu szybko się zwrócą. Otrzymują oni również prawo wstępu do salonu VIP, kompleksu odnowy biologicznej i masażu znajdującego się na miejscu. Posiadacze chipów są w mniejszym stopniu zagrożeni przez rabusiów i kieszonkowców, nie grozi im również utrata karty kredytowej.

²³² Pochodzenie terminu „brandscape” (krajobraz marek) Brytyjska Rada Wzornictwa (Design Council) definiuje następująco „Całkowity eksperymentalny zasięg i zaangażowanie marki. Termin ten obejmuje wszystkich, którzy stykają się i współoddziałują z marką, w tym klienci, dostawcy, pracodawcy, konkurenci, osoby odsprzedające, dystrybutorzy, partnerzy itp.”: http://www.design-council.org.uk/webdav/harmonise?Page/@id=6046&Session/@id=D_rPJLjJbFNakH0E0GQvlo&Document%5B@id%3D5232%5D/Chapter/@id=7.

²³³ To, którzy konsumenci są najcenniejsi, jest ustalane poprzez sprawdzenie karty kredytowej i porównanie z profilem klienta. Bycie wartościowym konsumentem oznacza zdolność do wydawania większych sum pieniędzy. Implanty stają się symbolem wysokiego statusu.

²³⁴ Patrz: Baja Beach „Zona VIP” <http://www.bajabeach.es/>.

²³⁵ Umożliwia to utrwalenie w bazie danych pewnych wyborów dokonywanych przez kolejne osoby.

- 30.2. Krążyły wprawdzie pogłoski, że niektórzy klienci zostali napadnięci na parkingu i że chipy zostały wycięte z ich ramion, ale kierownicy centrum zdementowali te opowieści jako „miejskie plotki”. Gareth zastanawiał się nad udziałem, ale zniechęciły go informacje podane w programie telewizyjnym, że chipy posiadają jedynie niski poziom zaszyfrowania i łatwo mogą zostać uszkodzone przez wirusy.²³⁶ Jednakże ludzie wolą chipy od kart kredytowych z innego powodu. Następstwa otrzymania wezwania w związku ze „znamionami nietypowej działalności” są obecnie znacznie poważniejsze. Z uwagi na znacznie bardziej zaawansowane algorytmy prognostyczne, oparte o indywidualny profil klienta, otrzymanie wezwania z banku postrzegane jest jako równoznaczne z byciem winnym. Karty są automatycznie dezaktywowane, a od konsumenta wymaga się dostarczenia bankowi niezależnych dowodów dotyczących jego tożsamości i miejsca pobytu. Jeżeli centrum handlowe zwróci się do klienta z prośbą o udzielenie informacji w takim samym celu, to otrzyma jedynie ogólne dane.

31. Mieć dzieci na oku

- 31.1. Do roku 2016 oznaczanie identyfikatorami i śledzenie przemieszczania się dzieci stało się zasadniczym elementem edukacji.²³⁷ Po serii głośniejszych przypadków zaginięcia, zranienia lub śmierci uczniów wiele szkół podstawowych, a nawet przedszkoli, aby uniknąć odpowiedzialności prawnej, zaczęło bardzo poważnie troszczyć się o kontrolę nad tym, gdzie przebywają uczniowie.²³⁸ W ciągu dziesięciu lat, w odpowiedzi na rządową politykę wczesnego wykrywania dzieci z problemami, zapobiegania zjawisku niskiej frekwencji i poprawy skupienia uczniów na lekcjach, coraz większa liczba szkół przyjęła rutynowe testy na obecność narkotyków.²³⁹
- 31.2. System bezgotówkowych kart w szkole Toby’ego zaczął już funkcjonować, przy czym większość rodzin używa go jako metody sprawdzania tego, co zjadły ich dzieci. Po trzech latach, supermarket NSC wykupił firmę obsługującą system bezgotówkowych kart, uznając to za sposób, dzięki któremu można dotrzeć na lukratywne rynki młodzieżowe, budując przy tym świadomość marki poprzez dostarczanie sprzętu naukowego. Aby otrzymać odpowiednie środki, rodzice muszą teraz wczytywać kartę swojego dziecka przy kasach. Karta ta zawiera informacje dotyczące szkoły, ucznia i rodzica. W ramach systemu finansowany jest sprzęt komputerowy, naukowy i sportowy oraz instrumenty muzyczne dla uczestniczących w nim szkół, pod warunkiem, że rodzice uczęszczających do nich dzieci dokonują zakupów w NSC. Wartość podarowanego sprzętu jest uzależniona od wartości zakupów dokonywanych przez rodziców. Niektórzy spośród głównych, związanych z koncernami produkującymi żywność i napoje, dostawców supermarketów NSC zaczęło ustawiać swoje automaty do sprzedaży w szkołach. Szkoła Toby’ego uczestniczy w systemie, a za każdym razem, gdy do szkoły przybywa nowy sprzęt, wyraźnie widoczny jest znak firmowy „NSC”.
- 31.3. Karta, o której mowa, ma również inne zastosowania. Lokalne władze odpowiedzialne za edukację monitorują rodzaje żywności spożywanej w szkole Toby’ego i wykorzystują je w trakcie rozmaitych kampanii „zdrowego odżywiania

²³⁶ Patrz.: Rieback, M.R., Simpson, P.N.D., Crispo, B. i Tanenbaum, A.S (2006) „RFID Viruses and Worms [Wirusy i robaki RFID]”, Department of Computer Science [Wydział nauk komputerowych] Vrije Universiteit Amsterdam, <http://www.rfidvirus.org/>.

²³⁷ W USA praktyka ta jest obecnie w powijakach. Patrz np: Leff, L. „Students ordered to wear tracking tags [Uczniowie, którym nakazano noszenie identyfikatorów umożliwiających ich śledzenie]”, *Associated Press*, 9 February 2005, <http://www.msnbc.msn.com/id/6942751/>.

²³⁸ Patrz np.: „Neglect ruling in girl pond death [Wyrok w sprawie utonięcia dziewczynki w stawie: zaniedbanie]”, *BBC News*, 23 March (23 marca) 2006, http://news.bbc.co.uk/1/hi/england/coventry_warwickshire/4837614.stm.

²³⁹ W Wielkiej Brytanii w tabelach ligi edukacyjnej szkoły systematyzowane są w zależności od wyników egzaminacyjnych ich uczniów.

się”. Kampanie te stanowią również element odpowiedzi na program edukacyjny realizowany przez Ministerstwo Obywatelstwa Edukacyjnego. Dzieje się tak dlatego, że karta stopniowo pełni coraz więcej powiązanych ze sobą funkcji i zawiera nie tylko dane na temat dokonywanych przez dziecko zakupów jedzenia, ale także jego frekwencji, rejestru osiągnięć, zajęć ponadprogramowych, wyników badań na obecność narkotyków i dostępu do Internetu. Wpisy z bazy danych związanej z kartą podlegają przedłożeniu jako dowód aktywności obywatelskiej ucznia. Podczas, gdy nasilenie się nadzoru w szkołach przynosi wymierne korzyści zarówno dla szkół, jak i dla samych uczniów, same dzieci stopniowo przyzwyczajają się do nadzoru nad ich ciałami, śledzenia miejsca ich pobytu i zdalnego monitorowania ich diety, jako do normalnych zjawisk.

32. Totalne rozwiązania społeczne?

- 32.1. W 2016 roku znacznie bardziej wyraźny stał się podział dzielnic mieszkaniowych na zamknięte wspólnoty prywatne, takie jak ta, w której mieszka rodzina Jonesów, patrolowane i monitorowane przez dobrze wyposażone, sieciowe firmy ochroniarskie i będące dawniej własnością komunalną tanie osiedla mieszkaniowe, takie jak Dobcroft Estate. Dla Jonesów, system kamer i system identyfikacji funkcjonujący na osiedlu i wokół niego sprawia, że koszty ubezpieczenia są minimalne.²⁴⁰
- 32.2. W Dobcroft Estate, praca Yasmin nigdy się nie kończy. Jej zespół, składający się z przedstawicieli wielu agencji, stał się podwykonawcą innego prywatnego konsorcjum o nazwie Kompletnie Rozwiązania Społeczne (Total Social Solutions - TSS). Firma Personal Behaviour Schemes – PBS²⁴¹), które stosowane są wobec każdego mieszkańca Dobcroft Estate od dnia jego narodzin²⁴² (niektórych wynajduje się jeszcze przed urodzeniem²⁴³).
- 32.3. Wiele osób, którym przyznano wyższy poziom PBS²⁴⁴, jak Wilson Green, posiada implanty oparte na technologii RFID, które są automatycznie rejestrowane przez czujniki zamontowane w ich domach oraz przy wejściach na osiedle.²⁴⁵ Wszczepianie implantów odbywa się teoretycznie w sposób dobrowolny, ale podobnie jak w przypadku systemów funkcjonujących w sklepach i szkołach, także i w tym przypadku udział jest opłacalny – do najbardziej istotnych korzyści należy skrócenie okresu obserwacji.

²⁴⁰ Stowarzyszenie Ubezpieczycieli Brytyjskich (Association of British Insurers - ABI) wezwało do tego w dużym raporcie dotyczącym mieszkalnictwa ABI „*Securing the Nation: The Case for Safer Homes* [Zabezpieczyć naród: przykład bezpieczniejszych domów]”, London: ABI, 12.
<http://www.abi.org.uk/BookShop/ResearchReports/Securing%20the%20Nation%20July%202006.pdf>

²⁴¹ W tym miejscu przewiduje się, że mechanizmy Anti-Social Behaviour Orders (zakazów dotyczących zachowań antyspołecznych) i Intensive Supervision (intensywnego nadzoru) itp. (patrz: Crime and Justice Expert Report [Specjalistyczny raport w sprawie przestępczości i wymiaru sprawiedliwości]) ulegną standaryzacji i przybiorą postać Personal Behaviour Schemes (schematy zachowań osobistych) dla osób odpowiadających określonym wzorcom ryzyka dotyczącego wykroczeń. Ponieważ wszyscy mieszkańcy Dobcroft Estate spełniają co najmniej jedno kryterium poprzez sam fakt zamieszkiwania na osiedlu, na którym istnieje duże prawdopodobieństwo popełnienia przestępstwa, wszyscy podlegają systemowi PBS.

²⁴² Patrz n. 191

²⁴³ Tak zwana „biokryminologia” lub aspekty genetyczne zachowania przestępczego, obecnie na nowo cieszy się rosnącym zainteresowaniem. patrz np.: Rose, D. (2006) „Lives of crime [Życie w przestępczości]”, *Prospect* 125 (sierpień), http://www.prospect-magazine.co.uk/article_details.php?id=7604. Aby zapoznać się z wcześniej napisaną krytyką tej metody, patrz: Rose, N. (2000) „Biologia przewinienia: tożsamość patologiczna i zwalczanie przestępczości w kulturze biologicznej”, *Theoretical Criminology* [Kryminologia teoretyczna], 4 (1), 5–34.

²⁴⁴ Do roku 2016 więzienie stało się tylko kolejnym poziomem PBS. Prace społeczne, nadzór sądowy i więzienie stanowią jeden ciąg i w dużej mierze są zarządzane przez jednostki prywatne.

²⁴⁵ Rzekomo w celu poprawy bezpieczeństwa mieszkańców, w 2010 roku osiedle Dobcroft Estate zostało otoczone ogrodzeniem, w którym pozostawiono jedynie cztery wejścia i wyjścia, monitorowane przez funkcjonariuszy wsparcia lokalnego, kamery i czytniki RFID.

32.4. Obecnie całe Dobcroft Estate jest objęte jedną z tymczasowych „miejscowych godzin policyjnych” po tym, jak „młodzieńcy” z osiedla zostali rzekomo zidentyfikowani przez starszą kobietę z Sunnyview Retirement Village (osiedla dla emerytów, gdzie mieszka również Geeta), jako sprawcy szkód. Kobieta ta zaobserwowała podejrzaną zajście za pośrednictwem kamer wideo miejscowego systemu nadzoru. Obrazy przekazywane przez kamery można oglądać na lokalnych kanałach ochrony w telewizji cyfrowej, gdzie prezentowane są również zdjęcia „czarnych charakterów” – tych którzy naruszyli zasady przypisanego im PBS.²⁴⁶ W osiedlach mieszkaniowych systemy CCTV w przestrzeni publicznej niemal całkowicie uległy przekształceniu w telewizję otwartą (Open-Circuit Television – OCTV). Wszystkie osoby w wieku poniżej 18 lat otrzymały w związku z tym zakaz wchodzenia na teren osiedla lub jego opuszczania w godzinach od 18.00 do 6.00. Dla Sary oznacza to, że aby spotkać się ze swoją najlepszą przyjaciółką, Aleeshą, poza godzinami nauki szkolnej, jedna z nich musi zaryzykować spotkanie z uzbrojonymi w paralizatory (tasery) strażnikami osiedlowymi, którzy mają zwyczaj najpierw strzelać, a później zadawać pytania.

33. Zmiana zasad jazdy

33.1. Gdy Gareth wyjeżdża poza obszar osiedla, brama z kutego żelaza rozsuwa się automatycznie, a system rejestruje numery z tablicy rejestracyjnej, dokładny czas wyjazdu oraz liczbę i tożsamość osób znajdujących się w wozie. System ANPR osiągnął zasięg ogólnokrajowy w roku 2008 i obecnie na drogach jest tyle kamer, że próby zgadywania przy pomocy map i czujników, gdzie są zainstalowane, są bezcelowe.

33.2. Podręczny komputer, który Gareth podłącza do samochodu²⁴⁷ połączony jest z satelitarnym systemem globalnej nawigacji Galileo²⁴⁸ oraz państwowymi kamerami monitorującymi natężenie ruchu drogowego, co pozwala na znalezienie najszybszej trasy dojazdu. Znalezienie najkrótszej trasy wiąże się również z mniejszymi kosztami, ponieważ liczba przejechanych przez samochód kilometrów automatycznie obciąża konto bankowe Garetha za pośrednictwem systemu ANPR.²⁴⁹

34. Przyjazne, latające oczy na niebie

34.1. Duże obszary miast, podobnie jak granie, centra handlowe i szkoły, znajdują się pod silniejszym nadzorem, niż mogłoby to się wydawać na pierwszy rzut oka. Bezpieczeństwo stało się elementem estetyki otoczenia – systemy nadzoru zostały wkomponowane w architekturę i infrastrukturę. Stały się niewidoczne, ale jednocześnie – wszechobecne.²⁵⁰ Wiele ważnych budynków, należących do instytucji państwowych, które po 2001 roku były otoczone betonowymi zaporami, teraz znów wydaje się pozbawionych zabezpieczeń. Zamiast barykad strzeże je system różnych czujników, połączonych z niemożliwymi do sforsowania,

²⁴⁶ Mechanizm taki został wprowadzony eksperymentalnie w Shoreditch, dzielnicy Londynu. Został natychmiast ochrzczony nazwą „ASBO TV”. patrz np.: Swinford, S., „Asbo TV helps residents watch out [Asbo TV pomaga mieszkańcom pilnować się]”, *Times Online*, 8 January (8 stycznia) 2006, <http://www.timesonline.co.uk/article/0,,2087-1974974,00.html>.

²⁴⁷ W 2016 roku większość ludzi posiada takie urządzenia, które posiadają roamingowy, bezprzewodowy dostęp do internetu, usługi telefoniczne, system nawigacji komputerowej i inne funkcje. Funkcja nawigacji zapewnia również, że urządzenia (a w związku z tym i ich posiadacze) są możliwe do śledzenia.

²⁴⁸ Galileo jest europejską cywilną alternatywą dla amerykańskiego wojskowego systemu GPS. Pierwszy satelita został wystrzelony w 2004 roku, a niektóre usługi będą dostępne w 2008 roku, patrz : „Galileo, European Satellite Navigation System [Galileo, Europejski system nawigacji satelitarnej]” CEC Directorate General Energy and Transport (Dyrekcja Generalna Rady UE ds. Energii i Transportu), http://ec.europa.eu/dgs/energy_transport/galileo/intro/future_en.htm.

²⁴⁹ Istnieje wiele potencjalnych systemów: Patrz: np.: Independent Transport Commission (Niezależna Komisja Transportu) (2006) *Paying to Drive* [Płacić aby jechać] http://trgl.civil.soton.ac.uk/itc/p2d_main.pdf.

²⁵⁰ Patrz: Infrastructure and Built Environment Expert Report. [Specjalistyczny raport w sprawie infrastruktury i zabudowy].

automatycznymi zaporami, które – jeśli nie są akurat potrzebne – chowają się w podłożu.

34.2. Gdy Ben i Aaron udają się do centrum Londynu, aby wziąć udział w antywojennym proteście, są obserwowani przez małe, zdalnie sterowane samoloty szpiegowskie – bezzałogowe pojazdy powietrzne (Unmanned Aerial Vehicles – UAV).²⁵¹ Zostały one po raz pierwszy zastosowane w czasie igrzysk olimpijskich w 2012 roku, ale nie wycofano ich później z użytku. „Sukces” „przyjaznych, latających oczu na niebie”, jak nazwał te maszyny rząd,²⁵² został uznany przez burmistrza za główny powód dla ich dalszego ogólnego zastosowania.²⁵³ Ludzie niemal przestali już je zauważać.

34.3. Systemy CCTV również mniej rzucają się w oczy. Mniejsze kamery wbudowane są na wysokości oczu w słupy latarni ulicznych oraz w ściany, co umożliwia skuteczniejsze działanie powszechnie już stosowanych systemów rozpoznawania twarzy.²⁵⁴ Wypróbowuje się też oprogramowanie do odtwarzania kształtów, które przetwarza obrazy uzyskane z wieloobiektywowych kamer w obraz trójwymiarowy. obrońcy praw człowieka i prawnicy dowodzą jednak, że system ten jest niedokładny, a obraz nie jest „prawdziwy”.

34.4. System nie składa się wyłącznie z kamer. Niemal powszechne już stosowanie technik bezprzewodowych sprawia, że kamery są niezależne od wielkich skrzynek i systemów kabli. Dodatkowo, kamery połączone są z inteligentnym systemem oświetlenia ulic, który zapewnia teraz „idealne” warunki oświetlenia dla oprogramowania rozpoznającego podejrzanych oraz z uruchamiającymi się pod wpływem ruchu reflektorami. Wspomagają je dodatkowe kamery, uruchamiane w przypadku gęstego tłumu lub niezwyklego natężenia ruchu.

35. Niezidentyfikowana pod-klasa

35.1. Po proteście, który miał miejsce w 2016 roku, Ben i Aaron zostają zatrzymani przez prywatną firmę ochroniarską, zatrudnioną przez Westminster Business Improvement District (Westminster – Dzielnica Sprzyjająca Przedsiębiorczości).²⁵⁵ Strażnicy są zdalnie nadzorowani przez operatorów z policji, za pośrednictwem

²⁵¹ Samoloty klasy UAV od kilku lat używane są przez amerykańskie siły zbrojne. Obecnie najlepiej znanym przykładem jest zdalnie sterowany samolot „Predator”, używany w Iraku, patrz: „Predator RQ-1 / MQ-1 / MQ-9 Unmanned Aerial Vehicle (UAV), USA [Bezzałogowy Pojazd Powietrzny Predator RQ-1 / MQ-1 / MQ-9]”, *airforce-technology.com*, 2006, <http://www.airforce-technology.com/projects/predator/>. W Wielkiej Brytanii proponowano wiele rodzajów zastosowań, patrz: Jha, A., „On the horizon ... pilotless planes as fishermen's and firefighters' friends [Na horyzoncie... Bezpilotowe samoloty jako przyjaciele rybaków i strażaków]”, *The Guardian*, 30 August (30 sierpnia) 2006, <http://www.guardian.co.uk/science/story/0,1860825,00.html>. W Los Angeles policja już prowadzi próby z małym, zdalnie sterowanym samolotem szpiegowskim, zwanym „SkySeer”: Bowes, P., „High hopes for drone in LA skies [Wielkie nadzieje związane ze zdalnie sterowanym samolotem na niebie Los Angeles]”, *BBC News*, 6 June (6 czerwca) 2006, <http://news.bbc.co.uk/1/hi/world/americas/5051142.stm>.

²⁵² Mianem „przyjaznych, latających oczu na niebie” określił w roku 1995 minister spraw wewnętrznych kamery przemysłowe CCTV, patrz: Campbell, D. (1995) „Spy cameras become part of the landscape [Kamery szpiegowskie stają się częścią krajobrazu]”, *The Guardian*, 30 January (30 stycznia): s. 6.

²⁵³ Duże zawody sportowe często bywały okazją do wypróbowywania i wdrażania nowych technologii nadzoru. Na przykład, aby dowiedzieć się więcej o systemie CCTV i Pucharze Świata 2002 w Japonii, patrz: Abe (2004) *op cit.*, n.161; a o CCTV i igrzyskach Olimpijskich w Atenach, patrz: Samatas, M. (2004) *Surveillance in Greece* [Nadzór w Grecji], Athens: Pella.

²⁵⁴ Patrz: Specjalistyczne raporty w sprawie wymiaru sprawiedliwości, infrastruktury i zabudowy. Jednym z poważnych problemów związanych z rozpoznawaniem twarzy był kąt widzenia kamer CCTV, patrz. np. g.: Introna, L. i Wood, D. (2004) „Picturing algorithmic surveillance: the politics of facial recognition systems [Obrazowanie nadzoru algorytmicznego: polityka systemów rozpoznawania twarzy]”, *Surveillance & Society*, 2(2/3): s.177-198.

²⁵⁵ Zarządzanie obszarami miejskimi już jest przekształcane w stosunki z zakresu partnerstwa publiczno-prywatnego lub organizacje zarządzania centrami miast (Town Centre Management) <http://www.atcm.org/> oraz dzielnic sprzyjających przedsiębiorczości (BID). Według rządu, rozwiązanie typu BID umożliwia „inwestowanie w lokalne środowisko handlowe poprzez świadczenie usług o wartości dodanej” <http://www.ukbids.org/>. W 2016 roku jednym z największych problemów dotyczących przepisów jest kwestia dzielenia się informacjami pomiędzy państwem a firmami ochroniarskimi działającymi w imieniu lub zamiast państwa. Szczególnie teraz Krajowy Komputer Policyjny łączy się z tak wieloma bazami danych, tak że policja, nadzór, więzienia i służby społeczne posiadają liczne wzajemne powiązania.

przenośnych, podręcznych komputerów²⁵⁶ i zamontowanych na kaskach mikrokamer, które rejestrują zatrzymanych chłopców.²⁵⁷ Paradoksalnie, to policjanci i funkcjonariusze bezpieczeństwa mają największe powody, aby mieć się na baczności, ze względu na stały monitoring. Oznacza to bowiem, że są stale kontrolowani i że utracili „elastyczność” reagowania.

35.2. Od Bena pobrana zostaje rutynowo próbka do analizy DNA, którą przeprowadza się natychmiast, podczas gdy Ben wręcza swoją kartę identyfikacyjną w celu dokonania odczytu. Gdy na ekranie pojawiają się dane, funkcjonariusz żartuje, że taki przeciwnik kapitalizmu właśnie wrócił z wakacji w Stanach Zjednoczonych.²⁵⁸ Ben uprzejmie odpowiada grymasem, przypominającym uśmiech.

35.3. Posiadanie karty identyfikacyjnej jest w dalszym ciągu teoretycznie dobrowolne i Aaron, który pochodzi z chrześcijańskiej rodziny, nie chce mieć takiej karty. Jego matka powiada, że taka karta to „znak bestii”, ale Aaronowi chodzi po prostu o to, aby zostawiono go w spokoju. Teraz dochodzi do wniosku, że wiąże się to z dużymi utrudnieniami, ponieważ: nieposiadanie karty oznacza, że skutecznie pozbawił się szansy ubiegania się o pracę na posadzie państwowej, otrzymywania korzyści lub kredytów studenckich, jak również podróżowania pociągami dalekobieżnymi lub samolotami nawet na terytorium Wielkiej Brytanii. Zaczyna się zastanawiać, czy było warto i jak teraz ma żyć. Słyszał wprawdzie o spółdzielczych projektach realizowanych na wsi, gdzie ludzie nie posiadają kart identyfikacyjnych, ale on jest chłopcem z miasta i boi się „odrzućcia”. A teraz grozi to jeszcze gorszymi konsekwencjami: jako młody, czarnoskóry mężczyzna bez karty, jest wysoce podejrzany i policyjne centrum dyspozycyjne nakazuje ochroniarzom doprowadzić go na dodatkowe przesłuchanie.²⁵⁹

36. Wirtualne śledzenie

36.1. Po zwolnieniu przez policję Ben idzie do swojego domu w Finchley, ale jego podręczny komputer jest już śledzony przez system Galileo²⁶⁰. Zostaje również umieszczony na liście osób, których połączenia będą teraz śledzone: jego ISP (dostawca usług internetowych) otrzymał automatyczny nakaz RIPA 2, aby wszelkie jego połączenia internetowe i cała poczta elektroniczna były zapisywane i przekazywane policji.²⁶¹ Ponieważ większość połączeń telefonicznych odbywa się teraz za pośrednictwem Internetu, a stare połączenia lądowe zanikają, nakaz ten obejmuje wszystkie połączenia i całą korespondencję Bena.

36.2. Jedną z konsekwencji takiego stanu rzeczy oraz faktu, że „właścicielami” Internetu są w dalszym ciągu firmy działające w USA, są ponawiane przez ruch

²⁵⁶ Wiele służb policyjnych wypróbowuje już takie urządzenia, patrz np.: „Pocket computers put police 'in the picture' [Komputery kieszonkowe doprowadzają policjantów „na miejsce”]”, *West Yorkshire Police*, 28 March (28 marca) 2006, <http://www.westyorkshire.police.uk/section-item.asp?sid=12&iid=2226>, i system „Airwave” (patrz: Crime and Justice Expert Report [Specjalistyczny raport w sprawie przestępczości i wymiaru sprawiedliwości]).

²⁵⁷ Umieszczone na kaskach kamery, przekazujące obraz w czasie rzeczywistym do centrów kontroli już obecnie są wprowadzane w niektórych miejscach: „Police use anti-yob head cameras [Policja używa noszonych na głowie kamer, aby zapobiec chuligańskim zachowaniom]”, *BBC News*, 23 March (23 marca) 2006, http://news.bbc.co.uk/1/hi/wales/north_east/4836598.stm.

²⁵⁸ Policja i jej prywatni sprzymierzeńcy mają dostęp do niemal każdej bazy danych podłączonej obecnie do Krajowego Komputera Policyjnego.

²⁵⁹ W 2016 roku wciąż toczą się spory w mediach i wśród polityków w sprawie takiego postępowania policji. Policja argumentuje jednak, że karty identyfikacyjne stanowią łatwy sposób określenia czyjejs dobrej woli (bona fides) i że nie może ponosić ryzyka związanego z założeniem, że osoba nie posiadająca karty jest niewinna.

²⁶⁰ Patrz n. 247.

²⁶¹ Obecna ustawa o regulacji uprawnień śledczych (Regulation of Investigatory Powers Act - RIPA) z roku 2000 zezwala na utrwalanie i zachowywanie zapisów w ograniczonym zakresie, ale zakładamy, że policja i służby bezpieczeństwa będą chciały „zaczynać pętlę”, najprawdopodobniej w odpowiedzi na jakiś bardzo głośny skandal związany z terroryzmem lub pedofilią. Doprowadzą do tego prawdopodobnie wraz z wejściem w życie nowej ustawy RIPA w 2009 roku.

Open Source („Otwarte źródło”) oraz przez inne wielkie kraje wysiłki na rzecz stworzenia „alternatywnych Internetów”. Do roku 2016 znalazły się wśród nich: znacznie silniej kontrolowany chińskojęzyczny projekt²⁶², który obecnie obejmuje swoim zasięgiem większą część południowo-wschodniej Azji, kilka ponadnarodowych wspólnych przedsięwzięć, m. in. „Googlenet”²⁶³ i znacznie większa liczba oferujących większą swobodę i „przejrzystość” projektów sieciowych.²⁶⁴

36.3. Jednym z nieprzewidzianych skutków wprowadzenia nadzoru nad połączeniami i pocztą Bena stało się objęcie monitoringiem Toby’ego, młodszego brata Bena, który od czasu do czasu korzysta z kont Bena (w głównej mierze tylko dlatego, że cieszy go włamywanie się na czyjeś konta). Toby spędza dużo czasu w sieci, grając w masowe wieloosobowe gry online (Massively Multiplayer Online Games - MMOG), wirtualnych światach, które rządzą się własnymi prawami i dysponują całymi alternatywnymi gospodarkami.²⁶⁵

36.4. Społeczeństwo nadzorowane dotarło także i tutaj. Zachowanie graczy w trakcie gry²⁶⁶ podlega monitoringowi ze strony firm, które starają się odnaleźć nowe możliwości dla nowych, kształtujących się w prawdziwym świecie rynków. Pojawiła się cała nowa kategoria uczestników gry – są nimi firmy. Gracze ci badają zwyczajnie ludzi z wykorzystaniem stworzonych przez siebie bohaterów i sprzedają innym graczom zarówno wirtualne, jak i prawdziwe produkty tak w wirtualnych światach, jak i poza nimi.²⁶⁷

36.5. Policja również zaczęła prowadzić doświadczenia z oprogramowaniem i monitoruje gry MMOG w celu zidentyfikowania takich osobowości i takich zachowań ich bohaterów (awatarów), które mogłyby wskazywać na zbrodnicze skłonności u kryjących się za nimi graczy.²⁶⁸ Takie podejście jest oczywiście odbierane bardzo kontrowersyjne wśród uczestników gier, którzy dowodzą, że eskapizmu światów wirtualnych nie należy mylić z prawdziwym życiem.

37. Twoje życie to nasza sprawa

²⁶² Projekt ten już od jakiegoś czasu jest w fazie rozwoju patrz : „China to launch ‘alternative’ Internet”, [Chiny zamierzają uruchomić „alternatywny” internet]” *New Scientist Technology Blog*, 1 March (1 marca) 2006, <http://www.newscientist.com/blog/technology/2006/03/china-to-launch-alternative-internet.html>.

²⁶³ Od 2005 roku krążą sprawozdania o ambitnych planach Google’a w tym kierunku, patrz. Np.: Hedger, J. (2005) ‘Is Google building an alternative Internet? [Czy Google buduje „alternatywny” internet ?]’ *SiteProNews* 23 września, przedruk w: <http://www.wnwdesign.co.uk/wordpress/archives/197>

²⁶⁴ Patrz np. Brin, D. (1999) *The Transparent Society* [Przejrzyste społeczeństwo], Reading MA: Perseus. <http://www.davidbrin.com/tschp1.html>

²⁶⁵ Gry MMOG, według niektórych szacunków mają obecnie około 13 milionów graczy. Największą z nich jest *World Of Warcraft*, <http://www.worldofwarcraft.com/index.xml> i koreańska rodzina gier *Lineage I*, <http://www.lineage.com/>, i *Lineage II*, <http://www.lineage2.com/>. Inne wirtualne światy są w większym stopniu analogiami świata rzeczywistego – należy do nich gra *Second Life*: <http://secondlife.com>. Ich charakter z czasem ulega pogłębieniu, a funkcjonujące w nich gospodarki w coraz większym stopniu przenikają się z prawdziwym światem. Przedmioty z gier są sprzedawane za „prawdziwe” pieniądze na takich stronach aukcyjnych, jak *ebay*, <http://www.ebay.com>. Aby zapoznać się z analizami statystycznymi, patrz *MMOGCHART.COM*, <http://www.mmogchart.com/>.

²⁶⁶ Mieszkańcy wirtualnych światów zazwyczaj są reprezentowani przez „awatara” – sieciową osobowość.

²⁶⁷ Już obecnie istnieją relacje na temat „wirtualnego nadzoru” patrz np.: „Confessions of a Virtual Intelligence Analyst [Wyznania analityka wirtualnego wywiadu]”, *Terranova*, 15 March (15 marca) 2006, http://terranova.blogs.com/terra_nova/2006/03/confessions_of_.html. Analitycy rynku już odkryli nowe rynki wirtualne o dużym znaczeniu, co oznacza że firmy zaczynają interesować się światami gier, patrz np.: Burns, E., „Marketing Opportunities Emerge in Online Gaming Venues [W grach sieciowych pojawiają się możliwości sprzedaży]”, *ClickZ*, 1 August (1 sierpnia) 2006, <http://www.clickz.com/showPage.html?page=3623035>, uruchomiono też pierwsze „wirtualne billboardy” patrz: Shields, M., ‘Massive Unveils Toyota Ad Units Within Anarchy’, *Mediaweek*, 19 July (19 lipca) 2006, http://www.mediaweek.com/mw/news/interactive/article_display.jsp?vnu_content_id=1002876380.

²⁶⁸ Doszło do tego po trwającej kilka lat serii zdarzeń, gdzie przestępstwa, do których doszło w grach MMOG, zostały powtórzone w rzeczywistości, patrz np.: „Chinese gamer sentenced to life [Chiński gracz skazany na dożywocie]”, *BBC News*, 8 June 2005 (8 czerwca), <http://news.bbc.co.uk/1/hi/technology/4072704.stm>.

- 37.1. Biuro obsługi klienta w 2016 r. pod pewnymi względami jest takie samo jak biuro obsługi klienta w 2006 r. Pracownicy są monitorowani w każdej minucie dnia za pomocą komputera, który rejestruje każdą czynność, którą wykonują, to jak długo ją wykonują i jak dobrze to robią. Metody rekrutacji i wynagradzania pracowników bardzo się różnią i ich cechą charakterystyczną są techniki nadzoru, które Gareth musi wprowadzić.
- 37.2. W czasie rekrutacji pracownicy są poddawani szeregowi testów biometrycznych²⁶⁹ i psychometrycznych oraz sprawdza się ich tryb życia. Ich życie poza pracą i ich pochodzenie są poddawane analizie. Wydaje się, że coraz większe znaczenie ma to, aby tryb życia pracownika i tryb życia klientów były zbliżone, ma to zapewniać lepszą obsługę klienta.²⁷⁰ Potencjalni pracownicy często obawiają się badań lekarskich, dlatego za namową agencji pośrednictwa pracy, które werbują pracowników dla biur obsługi klienta, zaczęli oni dobrowolnie podawać informacje o stanie zdrowia, żeby uniknąć badań. Aby zaoszczędzić czas obecnie rekrutujący odrzucają CV bez podanych informacji o stanie zdrowia.
- 37.3. Gareth bardzo wierzy w obecne zarządzanie dobrym samopoczuciem. W końcu jak zespół zarządzający może się cokolwiek dowiedzieć o tym, co powoduje mniejszą wydajność pracowników wykorzystując tylko szereg statystyk dotyczących wydajności?²⁷¹ Na przykład okresowe testy biometryczne informują pracodawcę o wszelkich problemach zdrowotnych, a także o tym, czy pracownik potrzebuje pomocy psychologicznej.²⁷² Dzięki współpracy z lokalnym klubem sportowym, który wykorzystuje ten sam system kontroli polegający na skanowaniu siatkówki jak biuro obsługi klienta, pracownicy mogą ćwiczyć za mniejszą opłatą. Ich aktywność sportowa jest rejestrowana w elektronicznych kartach pracy. Pracownicy, którzy nie uczęszczają regularnie do klubu sportowego są czasami pytani o tryb życia podczas ocen rocznych, szczególnie jeżeli ich wydajność w pracy była obniżona. Okresowe testy psychometryczne także pokazują dyrekcji czy postawa pracowników jest uznawana za zgodną z wartościami i kulturą firmy.
- 37.4. Praca biura obsługi klienta została podzielona na dwie części: najprostsze pytania i czynności administracyjne zostały zautomatyzowane lub są realizowane w krajach o niskich kosztach. Jednak niektóre zadania biura obsługi klienta wymagają bardzo złożonej pracy polegającej na sprzedaży osobistej. Dzięki danym karty nagród, łączeniu konsorcjów i sprzedawaniu szczegółowych informacji dotyczących profilu konsumentów, biura obsługi klienta zapewniają kompleksową obsługę najbardziej wartościowym klientom. Kiedy konsument dzwoni w sprawie danego produktu, komputer pracownika wyświetla cały profil konsumenta. Pracownik może wówczas zapytać konsumenta o inne produkty, przeprowadzić ocenę zdolności kredytowej online i od razu zaoferować rabaty. Taki rodzaj sprzedaży, kiedy dysponuje się dużą ilością informacji na temat danego klienta, Gareth nazywa „zbliżeniem się do klienta”. Uważa, że jest to najlepsze rozwiązanie dla pracy biura obsługi klienta,

²⁶⁹ Testy biometryczne, które obejmują wymazy z jamy ustnej i próbki z moczu, które może łatwo zanalizować zatrudniona na miejscu pielęgniarkę za pomocą taniego zestawu, to środek umożliwiający pracodawcy łatwą ocenę tego, czy potencjalny pracownik stwarza zagrożenie dla wydajności, ponieważ test ostrzega pracodawcę o ewentualnych problemach ze zdrowiem. Umożliwia to także organizacji opracowanie elastycznego pakietu świadczeń dla danego pracownika, poprzez określenie różnych wartości dla ubezpieczenia zdrowotnego w zależności od stanu zdrowia pracownika.

²⁷⁰ Minusem tego jest to, że organizacja zatrudnia tylko określony rodzaj osób i stąd ma mniej zróżnicowany personel, zob. Raport ekspertów w sprawie nadzoru w miejscu pracy (*Workplace Surveillance Expert Report*).

²⁷¹ Stwierdzenie to ma podkreślić, jak kierownictwo uczestniczy w obecnej tendencji do „mierzenia niemierzalnego” – pracy, postaw, zdrowia i kultury.

²⁷² Na przykład w razie problemów z alkoholizmem, jeżeli poziom alkoholu we krwi jest zbyt wysoki, co wykazałoby badanie moczu.

bardziej satysfakcjonująca praca dla pracownika i bardziej spersonalizowana obsługa najbardziej wartościowych klientów.

38. Troska o ciebie

- 38.1. Sunnyview Retirement Village jest przekształconym i prywatnie zarządzanym osiedlem mieszkań komunalnych, w których 74-letnia Geeta mieszka od kilku lat. Chociaż mieszka sama, czuje się bardzo pewnie, bo w pełni korzysta z lokalnego systemu opieki „Telecare”. Oprócz czujników ruchu w każdym pomieszczeniu, w wannie jest wbudowane urządzenie kontrolujące uderzenia serca, w toalecie znajduje się urządzenie, które mierzy poziom cukru we krwi, w kuchni znajdują się czujniki, które wykrywają wyciek gazu, pożar lub zalanie. Geeta ma specjalny przycisk połączony z centralą telefoniczną władz lokalnych, które w razie jego naciśnięcia natychmiast dzwonią i sprawdzają, co się dzieje.
- 38.2. Obecność czujników i kamer w całym jej domu oznacza, że jej rodzina wie, że jest bezpieczna i dlatego odwiedza ją rzadziej niż kiedyś, co powoduje u niej uczucie samotności. Geeta uważa jednak, że skanery RFID w jej lodówce i szafkach są bardzo przydatne. Zawsze kiedy brakuje jej produktów spożywczych, komputer zarządzający jej gospodarstwem domowym zamawia produkty z lokalnego supermarketu przez Internet. Zamawiając dostawę do domu nie musi niepotrzebnie chodzić do sklepów.
- 38.3. Teraz jest także przyzwyczajona do badań dla kobiet. Musiała nawet poznać pielęgniarkę, Anitę, która jest córką jednego z jej sąsiadów. Badania obejmują te same testy co w 2006 r.: pobieranie próbek krwi i moczu, kontrola wzrostu, wagi, ciśnienia krwi i wzroku. Na szczęście Geeta cieszy się dobrym zdrowiem.
- 38.4. Jednak nie jest zwolenniczką masowych zmian w badaniach przesiewowych, które są prowadzone potajemnie. Bez jej wiedzy szpital, który analizuje jej wyniki rutynowo teraz wykorzystuje komputery do analizy mammogramów i dzięki ogromnemu rozwojowi baz danych pacjentów wyniki Geety są porównywane z wynikami innych kobiet w jej wieku z każdej innej placówki zdrowotnej w kraju.²⁷³ Baza danych umożliwia także specjalistom wyodrębnienie czynników ryzyka związanym z wieloma chorobami, pod kątem których była badana, więc statystyczne prawdopodobieństwo wystąpienia u niej na przykład zawału serca jest przewidywane z dużo większą dokładnością. Lokalna poradnia zdrowia kobiet stale udziela Geecie porad na temat diety, ponieważ znajduje się ona w grupie wysokiego ryzyka wystąpienia chorób serca.
- 38.5. Jest tak także w przypadku wielu innych kategorii ryzyka wystąpienia chorób powszechnych. Między znacznie szerszym zakresem dolegliwości a ich wskaźnikami tworzy się statystyczny związek przyczynowy. Większe proporcje populacji są rutynowo dzielone na kategorie i badane, co wsparło badania statystyczne. Yasmin często skarży się na to, że Gareth opuszcza badania dla mężczyzn, ponieważ jak wielu mężczyzn bardzo niechętnie chodzi do lekarzy. Zastanawia się, jak wielu innych ludzi jak on bierze na poważnie stałą konieczność badań.
- 38.6. Statystycy służby zdrowia chętnie także posługują się danymi, aby potwierdzić swoją hipotezę, że dieta ma ogromne znaczenie dla zdrowia narodu. Mają jednak trudności. Dysponując krajową bazą danych pacjentów, która już istnieje i właściwie

²⁷³ Zob. np.: „The future of screening [Przyszłość badań przesiewowych]”, *BBC News*, 14 grudnia 2002, <http://news.bbc.co.uk/1/hi/health/2570787.stm>.

funkcjonuje, NHS (*National Health Service*) ciągle odmawia towarzystwom ubezpieczeniowym dostępu do informacji o stanie zdrowia wyłącznie w celach informacyjnych mimo pokusy zarobienia na tym ogromnej ilości pieniędzy. Kierownictwo NHS czuje, że dla zasady nie może prosić o dostęp do informacji na temat konsumpcji prywatnej. Ciągle obawia się skandalu takiego jak na Islandii, która sprzedała krajową bazę danych informacji o DNA prywatnym firmom na potrzeby prowadzenia badań i dla prywatnego zysku.²⁷⁴

39. Wnioski : lustrzany korytarz

- 39.1. Podczas gdy w 2016 r. nadzór ma większy zasięg, obywatele, szczególnie ci na tyle wykształceni lub zamożni, aby go docenić lub sobie na niego pozwolić, są w coraz większym stopniu świadomi jego obecności i potrafią znaleźć nowe sposoby negocjowania ich własnej osobistej gospodarki informacją. Gareth korzysta z usługi zarządzania informacjami osobistymi, która polega na monitorowaniu jego danych online. Automatycznie poprawia niepoprawne informacje znajdujące się w publicznych i niektórych konsumenckich bazach danych i uprzedza o innych problemach.
- 39.2. Niestety nie każdy może zmienić albo uzyskać dostęp do danych osobowych w równym stopniu. Osoby mniej biegłe w zarządzaniu danymi osobowymi lub mające mniej możliwości zapłacenia innym za zarządzanie ich danymi znajdują się w znacznie mniej korzystnej sytuacji. Możliwość blokowania przez urządzenia tych wiadomości (która jest wbudowana w droższe modele) ma duże znaczenie dla tych, którym zależy na prywatności i chcą dokonywać względnie niezależnych wyborów konsumenckich.
- 39.3. Cyfrowa przepaść powiększyła się, skazując niektórych na nadzór i brak możliwości uzyskania dostępu do informacji. Zwolennikom wolnego oprogramowania udało się ułatwić dostęp do gromadzonych przez państwo i firmy prywatne pracujące dla państwa danych osobowych i wprowadzanie w nich zmian, ale ten dostęp jest jedną z wielu rzeczy uwarunkowanych posiadaniem dowodu tożsamości. Coraz bardziej niepokojący i dotąd nierozwiązany jest konflikt między obywatelami a państwem dotyczący tego, kto co wie, kto posiada dane i kto ma prawo wprowadzania do nich zmian.
- 39.4. Ale w 2016 r. ludzie są bardziej przyzwyczajeni do obserwowania i bycia obserwowanymi. Wielu ludzi dobrowolnie prowadzi nadzór całego życia lub rejestrowanie życia, czyli zapisywanie prawie wszystkiego, co robią i przechowywanie tego lub umieszczanie bezpośrednio online²⁷⁵ w czasie rzeczywistym. To, co stanowiło subkulturę w 2006 r., zaczyna dominować w 2016 r.
- 39.5. Jednak kultura nadzoru wzajemnego także rozprzestrzeniła się i dała początek nowym wariantom. Duże znaczenie ma nadzór obywatelski prowadzony przez twardogłowych, którzy uważają, że państwo niedostatecznie zwalcza terroryzm, przestępczość i nielegalną imigrację²⁷⁶, mnożą się nieoficjalne strony internetowe na temat „elementów podejrzanych”, co prowadzi do różnych pomyłek błędnych

²⁷⁴ McKie, R., „Icelandic DNA project hit by privacy storm [Islandzki projekt DNA tematem awantury o prywatność]”, *The Observer*, 16 maja 2004, <http://observer.guardian.co.uk/international/story/0,6903,1217842,00.html>. Zob. także: Rose, H. (2001) *The Commodification of Bioinformation: The Icelandic Health Sector Database [Uprzedmiotowanie bioinformacji – baza danych islandzkiego sektora opieki zdrowotnej]*, London: The Wellcome Trust. http://www.mannvernd.is/greinar/hilaryrose1_3975.pdf

²⁷⁵ Rejestrowanie życia oznacza tworzenie blogów internetowych. W tym celu tworzy się już wiele technologii; zob. np.: Ward, M. (2004) „Log your life via your phone [Bloguj o swoim życiu przez telefon]”, *BBC News*, 10 marca, <http://news.bbc.co.uk/1/hi/technology/3497596.stm>.

²⁷⁶ Zob. Borders Expert Report i np.: inicjatywa obywatelska US Minutemen: <http://www.minutemanproject.com/>

identyfikacji.”²⁷⁷ Przeciwnicy, artyści i nadrealiści grają z wszechobecnym nadzorem i sprzeciwiają się mu na wszystkie sposoby, w tym poprzez unieruchamianie urządzeń nadzoru publicznego²⁷⁸, wykorzystywanie technologii „nadzoru” i antynadzoru.²⁷⁹ Antykapitalistyczni aktywiści jak na przykład Ben i Aaron lubią spędzać sobotnie popołudnia na umieszczaniu łatwo przyczepnej folii aluminiowej i przekaźników mikrofalowych zasilanych małymi bateriami w wejściach do sklepów w celu zakłócenia sygnałów radiowych.²⁸⁰

- 39.6. Rejestrowanie życia nie jest także tym wszystkim, na co może wyglądać a dzięki coraz bardziej złożonemu zarządzaniu danymi i oprogramowaniu do produkcji filmów wideo życie może zostać dostosowane lub nawet całkowicie stworzone dla różnych celów od rozrywki do oszustwa. Na przykład Toby ma alternatywny cyfrowy cień (*data shadow*), który stworzył jego przyjaciel haker, cyfrowy cień jest kilka lat starszy od niego i dużo ciekawszy i lepiej wygląda! W 2016 r. jest coraz więcej całkowicie wirtualnych cyfrowych cieni, które nie mają odpowiedników w świecie rzeczywistym, co do których wydaje się, że istnieją i same są przedmiotem zarządzania informacjami i nadzoru on-line prowadzonego przez zautomatyzowane systemy pracujące w sposób niesłyszalny i niewidoczny, są mieszkańcami niekończącego się lustrzanego korytarza...

²⁷⁷ Pojawiło się to już w związku ze strachem przed pedofilią, czego efektem było zmuszenie pewnej lekarki pediatry do opuszczenia domu w 2000 r., zob. np.: Allison, R., „Doctor driven out of home by vigilantes [Lekarka wyrzucona z domu przez straż obywatelską]”, *The Guardian*, 30 sierpnia 2000, <http://www.guardian.co.uk/child/story/0,7369,361031,00.html>. Oceniamy po prostu, że w 2016 r. technologie spowodują zwiększenie skali takich pomyłek.

²⁷⁸ Poradniki dotyczące takiego oporu już się pojawiły; zob. np.: „Guide to Closed Circuit Television (CCTV) destruction [Jak zniszczyć telewizję przemysłową]”, *Schnews*, <http://www.schnews.org.uk/diyguide/guidetoclosedcircuittelevisioncctvdestruction.htm>.

²⁷⁹ Zob. Mann, S., Nolan, J. and Wellman, B. (2004) „Sousveillance: inventing and using wearable computing devices for data collection in surveillance environments [‘Podzór’ – wynalezienie i wykorzystanie przenośnych urządzeń liczących do gromadzenia danych w środowiskach nadzoru]”, *Surveillance & Society*, 1(3), 331–355.

²⁸⁰ RFID jest technologią opartą na linii widzenia, zob. np.: „RFID Technology [Technologia RFID]”, *RFID Centre*, <http://www.rfidc.com/docs/rfid.htm>.

Część D:

Regulowanie

społeczeństwa nadzorowanego

40. Wprowadzenie

40.1. Jak pokazano w części C, rodzina Jonesów jest nadzorowana każdego dnia i przy okazji licznych wydarzeń i czynności, a w 2016 r. może być w jeszcze większym stopniu włączona w proces nadzoru. Niektóre procesy nadzoru są dla nich korzystne i pomocne; inne mają niebezpieczne lub oparte na wyzysku konsekwencje dla szeregu wartości i interesów, które rodzina Jonesów jako zwykli obywatele uważa za ważne i które ich kraj uważa za ważne dla idei dobrego życia w demokratycznym społeczeństwie demokratycznie rządzonym zgodnie z zasadą państwa prawa. Przez większość czasu Jonesowie nie wiedzą lub nie rozumieją, co dzieje się lub może stać się z ich danymi osobowymi: co jest gromadzone, przetwarzane, selekcionowane i udostępniane. Przez większość czasu nie zajmują się oni tymi kwestiami, ale czasem sytuacja staje się dla nich niekorzystna i podejrzewają, że coś się stało z ich danymi, co będzie miało negatywne konsekwencje. Co według nich można z tym zrobić? Co można z tym zrobić i kto to zrobi, jeżeli nie Jonesowie? Co uzasadnia nadzór? Jak te kontrole można usprawnić, aby zapewnić uregulowania umożliwiające dorównanie przeciętnemu poziomowi reprezentowanemu przez Jonesów?

40.2. Nadzór wymaga regulacji. „Regulacje” nie oznaczają tylko instrumentów prawnych do kontrolowania systemów i czynności, ale także wszelkie techniki, które mają skutek regulacyjny²⁸¹: to znaczy takie, które wykorzystują zasady, w ten czy inny sposób, do nadzoru lub przetwarzania danych poprzez określenie limitów i kontroli. Może to czasami obejmować ułatwianie „dobrego” nadzoru poprzez zarządzanie nim zgodnie z zasadami, regułami i wymaganymi zabezpieczeniami z jednoczesnym zakazem działań, które nie należą do systemu technicznego lub regulacyjnego. Większość systemów służących do kontrolowania procesów informacyjnych dotyczących danych osobowych zostało opracowanych w kontekście ochrony danych w celu zabezpieczenia *prywatności*. Uwagi znajdujące się w niniejszej sekcji dotyczą przede wszystkim tych strategii. Ale regulowanie *nadzoru* może znów być czymś więcej. Ochrona prywatności może być pierwszą linią obrony przed niepożądanymi konsekwencjami nadzoru. Jako taka jest silna i odporna, mimo dzisiejszego załamywania rąk nad jej znaczeniem i kiwania palcem na jej opieszałość. Z drugiej strony, można powiedzieć, że ochrona nadzoru musi być zaplanowana odrębnie, ponieważ jej niepożądane konsekwencje dotyczą nie tylko naruszania prywatności oraz że pierwsza linia obrony, chociaż istotna, jest słaba. Uważamy, że obydwa te stanowiska sprawdzają się w teorii i że w praktyce ochrona nadzoru z dużym prawdopodobieństwem pokrywa się z doświadczeniem i infrastrukturą ochrony prywatności lub danych i jest wzorowana na nich. Jednak jak przedstawiono w znajdującym w niniejszym raporcie omówieniu regulacji dotyczących telekomunikacji, skuteczność konwencjonalnych zasad ochrony jest poważnym problemem w przypadku niektórych aplikacji i najważniejszych technologii. To jak dużo inwencji potrzeba do ochrony nadzoru i jak wiele z niej

²⁸¹ Baldwin, R. and Cave, M. (1999) *Understanding Regulation: Theory, Strategy and Practice*. Oxford: Oxford University Press.

będzie w istocie wymyślaniem tego samego, jest kwestią do szerszego omówienia poza niniejszym raportem, chociaż poniżej powrócimy do niej omawiając ocenę oddziaływania na prywatność. Pozostaje jeszcze kwestia tego, czy regulowanie nadzoru jest w ogóle możliwe.

40.3. Działania nadzorcze, które zostały omówione w innym miejscu niniejszego raportu potwierdzają występowanie konsekwencji dla prywatności i kilku innych ważnych wartości takich jak sprawiedliwość, godność, samostanowienie, integracja społeczna, bezpieczeństwo i inne. Wiele z tych wartości można chronić jeżeli chroniona jest prywatność. Pewne formy nadzoru zwiększają możliwość korzystania z tych wartości przez osoby, grupy i społeczeństwa i dlatego są one zgodne z tym, co większość ludzi oczekuje od życia w krajach demokratycznych, gdzie przestrzegane są prawa człowieka i swobody oraz interesy zbiorowe. Z drugiej strony wiele działań nadzorczych zagraża tym wartościom poprzez negatywne oddziaływanie na szereg miejsc: dom, praca, przestrzeń publiczna, relacje obywatela z państwem, zakupy, granice, przemieszczanie się i tak dalej. Powiązanie pomiędzy ryzykiem naruszenia prywatności a tymi praktykami występuje powszechnie, ale nie jest konieczne. Nowe technologie i nowe wykorzystanie starych technologii są obiecujące, a jednocześnie niebezpieczne, a przyszłe zastosowanie nowości – na przykład *ambient intelligence* i wszechobecne komputery – może mieć takie konsekwencje, których można jedynie się domyślać. Nasza historia łączy istniejące działania nadzorcze z życiem dość typowej rodziny prowadzącej dość typowy tryb życia, a dalsze teksty o niej przesuwają ją w rzeczywistość kilka lat później. Nie pokazano skutków regulacji nadzoru ani naruszania prywatności, nawet jeżeli jest to ważna kwestia działalności regulacyjnej w wielu krajach i na poziomie międzynarodowym oraz w wielu krajowych i międzynarodowych organizacjach. Wielu powiedziałoby, że skutki te mogą osłabnąć a nawet że systemy regulacyjne i strategie są skazane na porażkę, jeżeli nie są – a nawet jeżeli są – naprawiane.

40.4. Niniejsza sekcja raportu zajmuje się tymi kwestiami. Zastanawiamy się nad doświadczeniem w regulowaniu i oceniamy adekwatność tych wysiłków. Mamy świadomość, że mierzenie efektywności ochrony prywatności i regulowania nadzoru jest zadaniem bardzo dyskusyjnym²⁸², ale jeżeli niniejszy raport wywoła taką dyskusję, osiągnie jeden ze swoich celów. Sugerujemy także możliwe ulepszenia.

41. Co jest nie tak z regulowaniem?

41.1. Można stwierdzić, że regulowanie i kontekst dyskusji o prywatności i nadzorze w każdym kraju ma pewne wady. Wymieniając je nie mamy zamiaru krytykować żadnego kraju ani uczestnika regulacji; nie dążymy też do stworzenia żadnego „rankingu” międzynarodowego. Możemy jednak zidentyfikować co najmniej sześć obszarów problematycznych o charakterze ogólnym i kontekstowym:

- Dążono do tego, aby regulowanie było adekwatne, to znaczy odpowiadało rozwojowi technologicznemu, wdrożeniu i wykonaniu po fakcie.
- Regulowanie w dużym stopniu koncentrowało się na kwestiach technicznych i kwestiach zarządzania w oparciu o kodeksy praktyki, wypełnianie standardowych wymogów prawnych i stosowanie technologii służących ochronie życia prywatnego; pozostawiono niewiele miejsca na przewidywanie.
- Znaczną część uregulowań oparto na wąskiej koncepcji prywatności osobistej i jej wartości dla ludzi, (koniecznie) odzwierciedlając obecne myślenie

²⁸² Bennett, C. and Raab, C. (2006) *The Governance of Privacy: Policy Instruments in Global Perspective* [Zarządzanie prywatnością – instrumenty strategiczne w perspektywie globalnej], Cambridge MA: MIT Press, ch. 9.

decydentów, którzy często w sposób ograniczony widzą to, co leży w „interesie publicznym”.

- Regulowanie było szeroko dyskutowane i wdrażane poza debatą publiczną. Debatę miała miejsce w środowiskach eksperckich: na przykład w środowisku ochrony danych lub wykonywania prawa. Oznaczało to bardzo niewielkie zaangażowanie ze strony zwykłych ludzi w jedną z najważniejszych kwestii naszych czasów.
- Regulowanie często jest postrzegane, pod względem politycznym, jako niesłuszne obciążenie dla przedsiębiorców oraz państwa, hamujące inicjatywę, podejmowanie ryzyka i wydajność. W Wielkiej Brytanii miała miejsce wyraźna próba deregulacji lub „lepszego regulacji” w celu zmniejszenia obciążenia. Objęło to ochronę prywatności i kontrolę nadzoru wraz z odpowiednimi konsekwencjami dla zdrowia, bezpieczeństwa i środowiska, w efekcie trudniej było wprowadzać nowe lub bardziej rygorystyczne wymogi. Uznanie, że przedsiębiorcy i rząd mogą być gotowi wykorzystać wzrost zaufania publicznego i wydajności, które może zapewnić regulowanie, jest w praktyce bardzo niepewne, chociaż bardziej oczywiste w teorii.
- Dyskusja w mediach koncentruje się na skandalach dotyczących naruszenia prywatności, a także przedstawia utopijne i orwellowskie widzenie technologii nadzoru. Wyjątkowe historie są ważne, ale zbyt często zapomina się o złożonych kwestiach etycznych i społecznych dotyczących nadzoru. O nadzorze często mówi się w kontekście zwykłego związku przyczynowo-skutkowego („systemy CCTV zapobiegają przestępczości”) albo strachu („wszyscy będziemy kontrolowani”). Podobnie, alternatywne poglądy są odpięane za pomocą błędnych i niebezpiecznych argumentów: „jeżeli nie masz nic do ukrycia, nie masz się czego obawiać”.

41.2. Są to jedne z głównych ogólnych i specyficznych trudności, które można wyróżnić w dzisiejszym środowisku regulacyjnym; dalej zajmiemy się problemami dotyczącymi określonych mechanizmów regulacyjnych. Niektóre z ogólnych trudności i okoliczności mogą się zmienić, chociaż niełatwo trudnością, inne nie. Świat nadzoru i regulowania prywatności zdecydowanie nie jest bierny i jego wysiłki nie były podejmowane na darmo, chociaż pozostają poważne wątpliwości jeżeli chodzi o osiągnięcia w przeszłości i prognozy na przyszłość.

42. Obecny stan regulacji

42.1. W ciągu ostatnich trzydziestu pięciu lub więcej lat ochrona prywatności rozprzestrzeniła się na całym świecie jako odpowiedź wielu krajów i organizacji międzynarodowych na zauważone zagrożenie ze strony działalności sektorów publicznego i prywatnego, które to sektory często dysponują zaawansowanymi środkami technologicznymi do przetwarzania danych osobowych.²⁸³ W centrum tych zjawisk leżały pewne podstawowe zasady zawarte w różnych sformułowaniach wielu aktów prawnych i dokumentów oficjalnych. Zgodnie z nimi organizacja:

- musi być *odpowiedzialna* za wszystkie dane osobowe, którymi dysponuje;
- powinna *określać cele*, dla których dane są przetwarzane w momencie ich gromadzenia lub wcześniej;

²⁸³ „Przetwarzanie” jest tu definiowane zgodnie z art. 2 lit. b europejskiej dyrektywy o ochronie danych osobowych 95/46/WE i oznacza każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie.

- powinny gromadzić tylko dane osobowe za *wiedzą i zgodą* danej osoby (poza wyjątkowymi okolicznościami);
- powinna *ograniczyć gromadzenie* danych osobowych do tych, które są niezbędne do realizacji określonych celów;
- nie powinna wykorzystywać ani ujawniać danych osobowych w celach innych niż określone bez zgody danej osoby (zasada *celowości*);
- powinna *zachować* dane tylko tak długo, jak to konieczne;
- powinna zapewnić *dokładność, kompletność i aktualność danych osobowych*;
- powinna chronić dane osobowe za pomocą odpowiednich *środków bezpieczeństwa*;
- powinna być *otwarta* w zakresie swoich polityk i praktyk oraz nie powinna prowadzić żadnego tajnego systemu informacji;
- powinna umożliwić osobom, których dane dotyczą *dostęp* do ich danych osobowych oraz ich zmianę, jeżeli są niedokładne, niepełne lub nieaktualne.²⁸⁴

42.2. Przepojone tymi lub podobnymi zasadami bezpiecznego obrotu informacjami regulacje dotyczące naruszania prywatności i nadzoru zostały rozpowszechnione w formie ustaw ogólnych, ustaw skierowanych do określonych sektorów (np. telekomunikacja) lub form działalności (np. zestawianie danych) oraz dokumentów międzynarodowych i deklaracji na szczeblu globalnym i regionalnym, z których prawdopodobnie najważniejszą jest dyrektywa o ochronie danych osobowych 95/46/WE i dyrektywa 97/66/WE. Powołano, na szczeblu krajowym, ponadnarodowym, a nawet regionalnym, organy regulacyjne takie jak rzecznicy ochrony danych i prywatności. Ponadto, firmy prywatne, stowarzyszenia handlowe i organy publiczne opracowały własne kodeksy postępowania i protokoły, sklepy internetowe przyjęły politykę prywatności lub przedstawiły oświadczenia o ochronie prywatności. W niektórych krajach instrumenty prawne i pozaprawne dotyczące poufności regulują praktyki wykonywane w ramach określonych zawodów i przez osoby zajmujące się przetwarzaniem danych osobowych, które często podlegają szczególnej ochronie. Na mocy różnych form aktów prawnych nałożono kary i sankcje. Ostatnio rozwiązania technologiczne – technologie podnoszące poziom ochrony prywatności – były wykorzystywane do ograniczania, zapewniania anonimowości i innego ograniczania nadzoru z wykorzystaniem samej technologii. Obrońcy prywatności głośno i aktywnie ostrzegali przed niebezpieczeństwem, ujawniali praktyki i podnosili publiczną świadomość tego, jak nadzór i naruszanie prywatności może wpłynąć na ich życie. Media często reagowały na zagrożenia związane z nadzorem, nawet jeżeli same czerpią korzyści z obnażania prywatności znanych osób, a także „zwykłych” obywateli.

42.3. Podsumowując, wokół nadzoru i prywatności było dużo zainteresowania i aktywności, a grupa ludzi i organizacji zaangażowanych w to jest liczna i działa w wielu miejscach. Pozostaje jednak duża obawa, że nawet najlepsze wysiłki i wymienione wyżej zasady są za słabe wobec utrzymywania się coraz większego zaawansowania klasycznego, rutynowego wkraczania w prywatność w obszarze przedsiębiorczości, coraz bardziej wszechstronnego nadzoru prowadzonego za pomocą technologii telekomunikacyjnych oraz nowych strategii rządowych, które wiążą się z przetwarzaniem danych osobowych na potrzeby szeregu proaktywnych i prognostycznych podejść do rozwiązywania problemów społecznych opartych na przetwarzaniu dużych ilości danych osobowych. Ponieważ ludzie coraz więcej podróżują po świecie – w ramach podróży służbowych lub prywatnych, w celach imigracyjnych i poszukiwaniu azylu lub w celu popełniania aktów terroryzmu –

²⁸⁴ *op cit.* n.281, 12.

działania nadzorcze nabierają większego międzynarodowego, transgranicznego wymiaru.

- 42.4. Tendencje te przyczyniły się do samospełniającej się negatywnej postawy wyrażanej w powszechnym myśleniu – podtrzymywanym przez niektóre grupy interesu – że „prywatność już nie istnieje, należy się do tego przyzwyczaić”, co osłabia popularność publicznego, politycznego i biznesowego wsparcia, z którego mogło korzystać regulowanie i którego potrzebuje. Podobnie jest w przypadku postawy, która zawsze dąży do równowagi między kontrolą nadzoru a zapewnieniem bezpieczeństwa w czasach strachu, „równowagi”, w której ten drugi element zawsze musi przegrać. Istnieje ryzyko, że znacznie zmaleje znaczenie „racjonalnego oczekiwania prywatności”, które coraz bardziej definiuje ramy, w których regulowanie jest omawiane i promowane, ponieważ ludzie, w tym dzisiejsze dzieci, od których pobierane są odciski palców w szkole lub w celu wydania paszportu²⁸⁵, które są monitorowane przez interoperatywne rządowe bazy danych lub znakowane przez pełnych obaw rodziców w celu monitorowania ich działań dla celów bezpieczeństwa, „przyzwyczajają się” do coraz większego ograniczania ich wolności od nadzoru.
- 42.5. Niniejszy raport nie jest miejscem na szeroką dyskusję o podstawowych teoriach nadzoru, które obowiązywały w ciągu kilku ostatnich dziesięcioleci. Wiele osób badających nadzór wykazywało tendencję do kwestionowania przywiązania do prywatności i jej ochrony jako głównego obszaru, w którym nadzór wzbudza wątpliwości, ponieważ sama prywatność jest jedyną wartością, która jest zagrożona i w konwencjonalnym rozumieniu jest postrzegana jedynie lub głównie w kontekście indywidualnych praw i swobód, które można egzekwować na mocy prawa.²⁸⁶ Tworzenie praktycznego systemu kontroli nadzoru na słabej i być może zniszczonej podstawie ochrony prywatności informacji wielu osobom wydaje się błędne. Dla innych²⁸⁷ jednak prywatność i jej ochrona może zostać rozszerzona na inne sytuacje, w które można fizycznie ingerować i w przypadku których występuje asymetria między jednostką a nadzorującymi, jak w przypadku nadzoru video. Inny przykład, mobilne śledzenie z wykorzystaniem zaawansowanych technologii nadzoru poruszających się pracowników i innych osób może być i w pewnym sensie już jest regulowane poprzez stosowanie klasycznych zasad do działań organizacyjnych i poprzez stosowanie szeregu instrumentów regulacyjnych – opisanych dalej – w stanowczy i spójny sposób.²⁸⁸
- 42.6. Nie jesteśmy przekonani, że w poszukiwaniu rozwiązań regulacyjnych należy wylewać dziecko z kąpielą lub że zasady i systemy dotyczące prywatności nie mogą jak Kanut Wielki powstrzymać rzekomego rozprzestrzenienia się nadzoru. Szereg zasad ochrony danych zgodnych z bezpiecznym obrotem informacjami jest jedyną racjonalnie zbudowaną i praktycznie ukierunkowaną ramą etyczną dostępną obecnie.²⁸⁹ Przypuszczenia, że blisko czterdzieści lat ochrony prywatności było urojoną grą prawodawców, nadzorujących i innych, którzy zajmowali się niewłaściwymi celami albo że te cele już nie stanowią zagrożenia wydają się niewiarygodne. Wiele sukcesów w regulowaniu nadzoru środkami ochrony granicy

²⁸⁵ Doward, J. (2006) „Millions of children to be fingerprinted [Plany pobrania odcisków palców od milionów dzieci]”. *The Observer*, 30 lipca, http://observer.guardian.co.uk/uk_news/story/0,,1833407,00.html

²⁸⁶ Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life* [Społeczeństwo nadzoru – monitorowanie dnia codziennego], Buckingham: Open University Press; Lyon (2003) *op cit.* n.6.

²⁸⁷ np.: Dubbeld, L. (2004) *The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance* [Regulacje obserwacji – implikacje nadzoru wideo dla prywatności]. Enschede: Ipskamp Printpartners.

²⁸⁸ Bennett, C. (2005) ‘Surveillance, employment and location: Regulating the privacy of mobile workers in the mobile workplace’, in Hansson, S. and Palm, E. (eds.), *The Ethics of Workplace Privacy*. Brussels: P.I.E-Peter Lang.

²⁸⁹ Bennett, C. (2006) ‘The mobility of surveillance: challenges for the theory and practice of privacy protection’. Dokument przedstawiony na 56. dorocznej konferencji International Communication Association, Drezno, 19-23 czerwca, panel na temat *Indywidualne i społeczne perspektywy bezpieczeństwa w sieci*.

prywatności można przypisać istniejącym systemom ochrony utworzonym w systemach prawnych i między nimi, chociaż, aby mieć pewność, wynik nie jest równy a systemy nie mają takich samych możliwości. Tym samym, złudne może być przypuszczanie, że umowna sensowność ochrony prywatności i danych oraz praktyczne środki, które w związku z nią wprowadzono nadal może być skuteczna dziś i w przyszłości. W przyszłości, to, co nazwano „nowym nadzorem”²⁹⁰ obejmującym ostatnie technologie, połączy się z elementami „starego nadzoru” opartego na technologiach „wieku komputerów”. W świecie wszechobecnych komputerów, na przykład, trudno jest sprawdzić, jak szereg zasad dotyczących prywatności lub bezpiecznego obrotu informacją może skutecznie funkcjonować pod względem zdolności regulacyjnych, ale ich zastosowanie nie powinno być po prostu wykluczone.

42.7. Co więcej, nowe praktyki nadzoru obejmują w coraz większym stopniu dyskryminację i inne „zło” społeczne w sposób, który ma znaczny i niesprawiedliwy wpływ na szanse życiowe poza dziedziną samego naruszania prywatności, co ma konsekwencje przede wszystkim dla ludzi. Można więc twierdzić, że systemy regulacyjne dotyczące nadzoru i prywatności muszą zostać przemyślane i zmienione (co najmniej) tak, aby mogły wpływać na projektowanie, wdrażanie i skutki nowych, bardziej intensywnych i ekstensywnych technologii nadzoru. Ale nowy nadzór to nie tylko technologie. Można powiedzieć, że „problemem” systemów regulacyjnych nie jest tylko to, jak radzić sobie z technologiami, ale także jak wpływać na strategię i cele tych, którzy je tworzą i rozwijają i jak wpływać na społeczeństwa i ludzi, którzy im podlegają.

42.8. Prywatność można więc zachować, ale nie zdecydowano jeszcze o istnieniu regulacji dotyczących prywatności, które poznaliśmy w ciągu ostatnich trzydziestu sześciu lat, w sytuacji, gdy ujawnione zostaną nowe zagrożenia. „Nowe regulacje” mogą więc być potrzebne nie jako całkiem nowa społeczna i rządowa filozofia lub praktyka, ale jako odbudowa, która obejmuje elementy z niedalekiej przeszłości, które są wciąż mocne i prężne. W 1998 r. Gary T. Marx²⁹¹ twierdził, że model ochrony danych nie jest już odpowiedni i że potrzebne są dla niego szersze ramy zasad etycznych, aby objął nie tylko prywatność informacji, ale także nadzór w sposób bardziej konkretny. Zasady te znajdowały się modelu konwencjonalnym, ale musiały zostać wydobyte na światło dzienne i powiązane ze środkami, kontekstami i zastosowaniami danych uzyskanych drogą nadzoru. Zaproponował 29 pytań do zadania przy określaniu czy nadzór jest zgodny z zasadami etycznymi; twierdzimy dalej, że to określenie jest podobne do oceny oddziaływania na prywatność (PIA). O ile Marx nie określa systematycznie, które z zasad ochrony danych lub bezpiecznego obrotu informacją nadal są odpowiednie, a które nie ani jak wiążą się z jego pytaniami i zasadami, które reprezentują, zasady te raczej albo wcale nie nadają się na śmietnik.

43. Instrumenty regulacyjne: wady i zalety

43.1. Przeanalizujemy pokrótce i skomentujemy istniejący zestaw szerokich, częściowo kolidujących ze sobą kategorii instrumentów politycznych, które były wykorzystywane do ochrony prywatności i danych i dlatego mają także zastosowanie do szerokich obszarów nadzoru:²⁹²

43.2. Instrumenty międzynarodowe

²⁹⁰ Marx, G.T. (1998) 'Ethics for the new surveillance,' *The Information Society* 14 (3): 171-85.

²⁹¹ *ibid.*

²⁹² Szczegółowa typologia i dyskusja: Tavani (281) op cit. nr 60.

43.2.1. Europejska Konwencja Praw Człowieka i inne deklaracje międzynarodowe nadają ochronie prywatności moc prawną i moralną, która może odgrywać ważną rolę w ograniczaniu nadużyć związanych z nadzorem. OECD²⁹³, Rada Europy²⁹⁴ i UE²⁹⁵ w największym stopniu przyczyniają się do rozwoju zasad i reguł ograniczających ingerowanie w prywatność, szczególnie jeżeli chodzi o prywatność informacji. Te i powiązane z nimi dokumenty dały początek działalności w zakresie tworzenia i wdrażania prawa w znacznej liczbie krajów i systemów prawnych o mniejszej skali. Niektóre z tych instrumentów międzynarodowych zachowały swoje oddziaływanie moralne, chociaż wartość tej zalety jest obecnie wątpliwa. Niemniej działania na szczeblu międzynarodowym są w dużym stopniu odpowiedzialne za wysoką pozycję szeregu zasad, wymienionych wyżej, które wpływały na ochronę danych, a zatem na wiele działań związanych z nadzorem przez długi okres.

43.2.2. Zasady, o których była mowa wcześniej są częścią „modelu prywatności”²⁹⁶, który przejęliśmy i który jest widoczny w podejściach wielu krajów. Jest to przede wszystkim pochodna konstrukcja proceduralna, która trochę przesłania podstawowe, istotne etyczne rozważania – choć nie są one niewidoczne. Nakłada to na „administratorów danych” szereg wymogów proceduralnych dla ich czynności związanych z przetwarzaniem danych i dlatego daje wrażenie, że formalna zgodność będzie wystarczająca do usankcjonowania ich działań. Sprzyja to raczej schematycznej mentalności niż systemowemu i systematycznemu podejściu do realizacji wartości. Akty prawne dotyczące ochrony danych są napisane zgodnie z tą ograniczającą ramą, co pozostawia oficjalnym i innym ciałom odpowiedzialnym za nadzór zadanie wypełniania lub stosowania bardziej istotnych rozważań pochodzących czasem z praw człowieka i innych prawnych lub filozoficznych zasad jak proporcjonalność, konieczność, uczciwość, sprawiedliwość i tak dalej.

43.3. Akty prawne

43.3.1. Upowszechnianie się na całym świecie środków prawnych służących kontroli przetwarzania informacji osobistych postępowało szybko od lat 70. do dziś. Wiele krajów stworzyło sektorowe i ogólne akty prawne dotyczące ochrony danych i większość z nich ustanowiła pewną formę mechanizmu egzekwowania i nadzorowania. Ten drugi element w postaci rzeczników ochrony prywatności i im podobnych ma kluczowe znaczenie dla wysiłku na rzecz ochrony prywatności. Stany Zjednoczone pozostają poza „klubem” krajów, które mają obszerne przepisy tego rodzaju, co osłabia globalne wysiłki na rzecz uregulowania nadzoru powodując, że są chaotyczne i niepełne. Sektorowe i specyficzne akty prawne, które regulują na przykład nadzór video, zestawianie danych, dane ze spisu ludności lub wykorzystanie danych genetycznych mogą przynosić korzyści dla interpretowania praw, ale także mogą uchylać przepisy ogólne w przypadku bardziej pilnych kwestii interesu publicznego i polityki, co osłabia ochronę. W niektórych krajach dodatkowo istnieje prawo powszechne chroniące poufność, które reguluje niektóre rodzaje nadzoru lub ingerowania. Nadbudową prawną są zapewne prawa człowieka

²⁹³ OECD (1981) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* [Wtyczne w sprawie ochrony prywatności i ponadgranicznych przepływów danych osobowych]. Paris: OECD.

²⁹⁴ Rada Europy (1981) *Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja 108)*. Strasburg: Rada Europy.

²⁹⁵ Szczególnie dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Bruksela, Dz.U. L 281 [Dyrektywa UE o ochronie danych osobowych]

²⁹⁶ *op cit.* n. 281, ch. 1.

oparte na międzynarodowych deklaracjach i rzecznicy ochrony prywatności uznali je za podstawę prawa, które mają egzekwować. Skuteczność środków prawych i mechanizmy egzekwowania, takie jak agencje regulacyjne (np. rzecznicy ochrony prywatności i „organy nadzorujące” w rozumieniu UE) różnią się w zależności od charakteru przypadków, uprawnień i dostępnych sankcji, sposobu wykonywania zadań regulacyjnych, zasobów zapewnionych przez rządy na potrzeby tej działalności oraz zakresu spraw i problemów wymagających wykonywania kontroli regulacyjnej.

43.3.2. Żadne z tych warunków nie dają podstaw do zachowania optymizmu w kwestii wystarczającej ilości rozwiązań prawnych, ale potrzeba ich wprowadzenia nie pozostawia prawie żadnych wątpliwości. Zapewniają wyrównawczy zestaw ograniczeń praktyk nadzoru, które mogą być zaskarżone ze względów prawnych – takich jak przekazanie CIA szczegółowych informacji bankowych klientów w systemie SWIFT międzynarodowych transakcji finansowych – a nie tylko ze względu na szkodliwość, co samo w sobie może okazać się nieskuteczne. Ujawnia to słabe punkty wielu ustaw i mechanizmów ich wdrażania na polu przetwarzania informacji osobowych, na które od dawno narzekano, dlatego też krytycy mogą mieć powód do zniecierpliwienia z powodu rozwiązań prawnych, które mogą jedynie usankcjonować nadzór zamiast go uregulować.²⁹⁷ Co więcej, ustawy o prywatności i ochronie danych z pewnością nie regulują szerokiego wachlarza praktyk nadzoru, takich jak te stanowiące część współczesnych praktyk telekomunikacyjnych, i nie można interpretować ich szeroko w tym sensie. Istnieją także inne ustawy, a wśród nich wiele interesujących pod kątem egzekwowania prawa i zwalczania terroryzmu, które wypierają lub w inny sposób osłabiają ustawy o prywatności; jak już wspomniano wcześniej w niniejszym raporcie, dane telekomunikacyjne są szczególnie narażone w tej kwestii. Rola sądów i trybunałów w ustalaniu legalności praktyk informacyjnych służących nadzorowaniu była decydująca, mimo że nie zawsze odnosiły się one przychylnie do powodów prowadzenia nadzoru i naruszania prywatności w wąskich granicach. Dodatkowo szkoda, którą może wyrządzić nadzór indywidualnym osobom, grupom i całym społeczeństwom, nie wchodzi w zakres konsekwencji, którym poszczególne ustawy oparte na prawach mają zaradzić lub zapobiec.

43.4. Samoregulacja

43.4.1. Sektory lub przedsiębiorstwa, organy specjalistyczne i państwa opracowały liczne kodeksy postępowania lub praktyk, aby uregulować nadzór w wielu dziedzinach działalności, wliczając CCTV, działania profesjonalistów, monitoring w miejscu pracy i tym podobne. Istnieją także metody samoregulacji *online* stosowane przez handlowców, którzy działają przez Internet, w postaci oświadczeń prywatności, „szczelnych” programów i tym podobnych, popieranych przez organizacje, które za nich poręczają. Samoregulacja jest czasem zapisana w ustawach, tak jak kodeksy praktyk, które zamieszczono w ustawie Zjednoczonego Królestwa o ochronie danych z 1998 r. i dyrektywie UE 95/46/WE o ochronie danych z 1995 r. Jednak coraz częściej samoregulacja jest uznawana za lepszy sposób regulacji, ze względu na „niepowodzenie” ustaw, a

²⁹⁷ Flaherty, D. (1989) *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States* [Ochrona prywatności w społeczeństwach nadzoru: Federalnej Republice Niemiec, Szwecji, Francji, Kanadzie i Stanach Zjednoczonych]. Chapel Hill NC: University of North Carolina Press.

większa swoboda w działalności gospodarczej powinna być wspierana.²⁹⁸ Nazywana czasem „łagodną ustawą” lub „łagodną regulacją”, samoregulacja woli kodeksy od reguł prawnych i sprawozdawczość wewnętrzną od zewnętrznych kontroli. A mimo to trudno wyobrazić sobie istnienie kodeksów i tym podobnych bez uprzedniego i jednoczesnego istnienia ustaw lub instrumentów międzynarodowych, które stanowią źródła wszystkich norm i wytycznych, które zawierają kodeksy. Wiarygodność i skuteczność samoregulacji jako głównego narzędzia ograniczania nadzoru nie zostały jak do tej pory wykazane. A to rodzi uporczywe pytania o odpowiedzialność, nadzór i przejrzystość, do których z niechęcią odnoszą się „lisy dowodzące kurnikami” i na które nie można udzielić zadowalających odpowiedzi w ramach samej tylko samoregulacji. Komentarze na temat samoregulacji w obszarze telekomunikacji przedstawione w innych fragmentach niniejszego raportu pokazują, że istnieje wiele elementów zachęcających firmy do ignorowania kodeksów i tym podobnych; mówiąc bardziej ogólnie, sankcje, które mogą nałożyć związki handlowe, mogą nie być wystarczająco surowe, aby powstrzymać lub ukarać ich członków dopuszczających się naruszeń.²⁹⁹

43.5. *Technologie służące ochronie prywatności*

43.5.1. Kiedy krytycy nadzoru przedstawili silną argumentację przeciwko technologiom, na początku lat '90 zdano sobie sprawę, że technologie mogą same zapewnić silną kontrolę nad nadzorem lub naruszaniem prywatności. To nie oznacza, że „technologia jest neutralna”, ale że możliwości konkretnych technologii w zakresie prowadzenia nadzoru zależą od tego, jak są zaprojektowane i rozmieszczone. A zatem kodowanie danych osobowych przy okazji ich przechowywania lub przepływu przez domeny i inne granice może mieć różny zakres: od braku kodowania do bardzo dobrego kodowania, projekt sieci i „kodeks” oprogramowania mogą mieć wyraźny efekt regulacyjny,³⁰⁰ pliki „cookies” mogą być filtrowane, aby nie dopuścić do nakreślania profili. Tym niemniej liczne elementy zachęcają przedsiębiorstwa, rządy i twórców oprogramowania do zaniechania zamieszczania „technologii zwiększających ochronę prywatności” (PET) w swoich systemach lub do wprowadzania opłat lub innych ustaleń, do których muszą dostosować się jednostki, jeśli chcą móc z nich korzystać; lub nawet do zakazywania ich wykorzystania, tak jak w przypadku dobrego kodowania. Wielu z pewnością zgodziłoby się, że nie można niezawodnie uregulować nadzoru za pomocą „ustaleń technologicznych”.

43.5.2. Niektóre technologie PET są wbudowywane (lub co gorsza „przyśrubowane”) do systemów ICT, podczas gdy inne są dostępne dla obywateli i konsumentów, zwłaszcza, kiedy surfują po Internecie i dokonują transakcji, pod warunkiem, że mają taką wiedzę, są na tyle świadomi i na tyle im zależy, żeby ich użyć, a czasem potrzebują w tym celu także środków finansowych. Kodowanie, anonimowe wyszukiwanie w Internecie, urządzenia filtrujące, inteligentne urządzenia, narzędzia dające pierwszeństwo prywatności i tym podobne mogą funkcjonować niczym instrumenty wspierające jednostki. Zarówno same w sobie, jak i jako alternatywa dla innych instrumentów są

²⁹⁸ US Department of Commerce, National Telecommunications and Information Administration (NTIA) (1997) *Privacy and Self Regulation in the Information Age [Prywatność i samoregulacja w dobie informacji]*. Washington DC: Department of Commerce, NTIA.

²⁹⁹ *op cit.* nr 281, roz. 6.

³⁰⁰ Lessig, L. (1999) *Code and Other Laws of Cyberspace [Kodeks i inne ustawy dotyczące cyberprzestrzeni]*. New York NY: Basic Books.

silnymi rozwiązaniami w obliczu praktyk nadzoru *online*, a mimo to nie gwarantują ochrony.

43.6. *Samopomoc w ramach własnych możliwości*

43.6.1. To kolejna ogólna kategoria regulacyjna, w ramach której indywidualni obywatele lub konsumenci kontrolują przekazywanie własnych informacji, na przykład przez wykorzystanie technologii PET, uczestniczenie w transakcjach online dających wybór uczestniczenia w niektórych procedurach przetwarzania informacji, ale także wykorzystywanie wiedzy, poszerzanie świadomości i zachowanie czujności w odniesieniu do praktyk nadzoru i zagrożeń prywatności, które pojawiają się każdego dnia. To wszystko jest na wagę złota dla osób, którym zależy na ochronie i „kapitale kulturowym” – posiadają umiejętność i środki, aby zrozumieć, co się dzieje, oprzeć się pochlebstwom osób gromadzących informacje, przeczytać informacje drobnym druczkiem na stronach internetowych i czuć pewność siebie w przypadku kontrolowania nadużyć i domagania się zadośćuczynienia, gdy zagrożenia się ziszcza. W USA, przy braku organów regulacyjnych lub nadzorujących, samopomoc we własnym zakresie, w tym także podejmowanie działań prawnych, to jedna z dominujących metod regulacji prywatności, przy czym model ten spotyka się z licznymi krytycznymi opiniami. Inne systemy ochrony danych opierają się w pewnym zakresie na skargach jednostek składanych organom regulacyjnym i informacjach dostarczanych przez nich na temat wątpliwych praktyk.

43.6.2. Rozwiązania oparte na prawie własności i rozwiązania rynkowe najbardziej wyróżniają się spośród działań ochronnych w ramach samopomocy,³⁰¹ ale zostały także mocno skrytykowane.³⁰² Rozwiązania rynkowe oznaczają, że można zapłacić bądź ponieść dodatkowe opłaty za swoją prywatność i sprzedać swoje informacje. Chociaż rozwiązania oparte na „prawie własności” własnych odniesieniu do swoich danych mogą odegrać rolę w samopomocy, mogą być przy tym ograniczane, jeśli brakuje wyraźnego określenia własności w systemach informacyjnych lub w przypadku wykorzystania określonych technologii. Tym niemniej, chociaż utrzymuje się powszechnie, że osoby indywidualne powinny i mogą ponosić odpowiedzialność za własną prywatność i ochronę przed nadzorem, jedynie ich garstka jest prawdopodobnie w stanie sprawować samopomoc w takim zakresie, jaki może sugerować „odpowiedzialność”, bez konieczności stawiania szeregu koniecznych warunków, aby pomóc tym osobom realizować założenia samopomocy lub „osobistej struktury ochrony”. Osoby indywidualne mogą wyrazić życzenie, aby „pozostawiono je samym sobie”, skoro jedna z interpretacji „prywatności” dopuszczałaby taką możliwość, ale nie mogą sprawować kontroli „na własną rękę”.

43.6.3. A zatem takie są główne kategorie ograniczających nadzór instrumentów ochrony prywatności wykorzystywanych w dzisiejszych czasach. Kolejne możliwości są nieustannie rozważane i promowane. Umowy i wiążące reguły korporacyjne w zakresie przekazywania danych także były widoczne w arsenale

³⁰¹ *ibid.*; Rule, J. i Hunter, L. (1999) „Towards property rights in personal data” [W kierunku praw własności w odniesieniu do danych osobowych], w Bennett, C. i R. Grant (eds.) *Visions of Privacy: Policy Choices for the Digital Age* [Wizje prywatności: wybory polityczne w dobie cyfrowej]. Toronto: University of Toronto Press; Laudon, K. (1996) „Markets and privacy” [Rynki i prywatność]. *Communications of the Association for Computing Machinery* 39: 92-104.

³⁰² Schwartz, P. (2000) “Beyond Lessig’s Code for internet privacy: Cyberspace filters, privacy control and fair information practices” [Poza kodeksem Lessiga w zakresie prywatności w Internecie: filtry w cyberprzestrzeni, kontrola prywatności i uczciwe praktyki informacyjne], *Wisconsin Law Review* 2000: 743-88; Rotenberg, M. (2001) “Fair information practices and the architecture of privacy (what Larry doesn’t get)” [Uczciwe praktyki informacyjne i struktura prywatności (czego Larry nie rozumie)], *Stanford Technology Law Review* http://stlr.stanford.edu/STLR/Articles/01_STLR_1

bronii przeznaczonej do ochrony danych. Istotne są także inne, mniej specyficzne instrumenty czy raczej kategorie osób odgrywających ważne role we wspólnocie regulacyjnej, a wiele z nich ma w istocie decydujące znaczenie w ramach każdej z tych głównych grup lub obejmuje je wszystkie, wnosząc ogólny wkład dla całego społeczeństwa. Chodzi tutaj o działania:

- grup nacisku opowiadających się za prywatnością i brakiem nadzoru – wraz z częścią mediów – które szerzą świadomość w kwestii zagrożeń, monitorują sytuację i naciskają na rządy oraz przedsiębiorstwa, które uciekają się do nadzoru;
- technologów, którzy opracowują systemy nadzoru i informacji oraz których wykształcenie, wyszkolenie i przestrzeganie kodeksów praktyk może wpłynąć na świadomość ich pracodawców i kształt produktów;
- naukowców akademickich, których praca może naświetlić to, co się dzieje, wytłumaczyć, dlaczego tak się dzieje i opracować oraz sprawdzić teorie na temat miejsca i legalności nadzoru w społeczeństwach w przeszłości, teraźniejszości i przyszłości; w ten sposób przybliżając wiedzę specjalistyczną ogółowi.

44. Ogólne problemy dotyczące instrumentów

44.1. Dla celów omówienia można przytoczyć trzy najważniejsze problemy dotyczące istniejących praktyk prawnych. Dwa z nich są związane z *rozdrobnieniem* i *słabą koordynacją*. Jeden problem dotyczy głównych instrumentów, drugi zaś skomplikowanych szczebli jurysdykcyjnych, na których ma miejsce wykonywanie prawa. W obydwu przypadkach wyzwaniem stanowi projekt potencjalnie bardziej ujednoliconego i globalnego nadzoru, jakim może zostać obciążone obowiązujące prawo, zważywszy na prawdopodobieństwo utrzymywania się obecnych tendencji. W obu przypadkach należy postawić pytanie: w jaki sposób można naprawić taką sytuację? Innymi słowy, czy ogień można zwalczać ogniem? Jeżeli siły działające na rzecz zwiększenia nadzoru coraz bardziej dążą do połączenia i integracji, bez względu na to czy odbywa się to w danym kraju, czy na szczeblu międzynarodowym, jak dalece są zintegrowane instrumenty i poziomy wyrównujących działań ochronnych? Trzecim problemem jest stosowanie tych instrumentów wobec społecznych skutków nadzoru oraz być może w szczególności „nowego nadzoru”, poza ingerencją w prywatność lub w odniesieniu do nowych narzędzi. W przypadku wszystkich trzech problemów istnieje możliwość ponownego przeanalizowania wachlarza przepisów prawnych pod względem możliwości poprawy ich spójności i skuteczności. Całkowite wykonanie tego zadania wykracza poza zakres niniejszego raportu, jednakże może on stanowić pewną podstawę dla zidentyfikowania tych zagadnień. Istnieje również pole do rozważań nad możliwością oceny wpływu prywatności i nadzoru, która może nastąpić na dowolnym poziomie i w dowolnym zakresie, dziedzinie lub sektorze stosowania. Również w tym zakresie raport ogranicza się do wskazania problemu.

44.2. Jeśli chodzi o instrumenty, te określone powyżej są zazwyczaj postrzegane jako część zestawu narzędzi pozostających do dyspozycji mechanizmów regulacyjnych. Jednakże taka metafora nie odpowiada rzeczywistej lub oczekiwanej relacji występującej pomiędzy poszczególnymi narzędziami ani temu, w jaki sposób powinny zostać lepiej zintegrowane. Rzeczywiście, nieodpowiedni może wydawać się sam pomysł pożyczenia pojęcia „narzędzia”.³⁰³ Większość narzędzi w zestawie

³⁰³ *op cit.* nr.281, r. 8.

narzędzi funkcjonuje zazwyczaj niezależnie od siebie i mają one konkretne przeznaczenie. Z drugiej strony narzędzia regulacyjne nie są wcale niezależne, w rzeczywistości są w dużej mierze wzajemnie zależne, zwłaszcza jeżeli którekolwiek z nich ma optymalnie funkcjonować. Na przykład instrumenty międzynarodowe zależą od wdrożenia i procesu prawodawczego, jakie mają miejsce na poziomie krajowym. Ustawy zależą od zgodności regulowanej dziedziny; zgodności tej nie można zakładać automatycznie ze względu na trudny do zdefiniowania i zawoalowany charakter procesów objętych regulacją. Organy regulacyjne o niskich uprawnieniach potrzebują wsparcia środków przekazu i grup nacisku, aby zwrócić uwagę na nadużycia w zakresie nadzoru, a także członków społeczeństwa, którzy mogą zgłaszać skargi, na podstawie których mogą wszczynać dochodzenia. Potrzebują ponadto ogólnego wsparcia politycznego i administracyjnego od systemów rządowych, w ramach których funkcjonują, od swoich odpowiedników organów regulacyjnych w innych jurysdykcjach oraz od sektorów biznesowych, które regulują i zachęcają do poprawy praktyk.

44.3. Ze swojej strony samoregulujące kodeksy praktyki mogą być bardziej skuteczne, jeżeli na podstawie obowiązujących ustaw i wymogów określonych przez organy regulacyjne dąży się do powołania mechanizmów współregulujących. W zamian za to można wymagać, aby uczestniczące w nich organizacje (np. firmy tworzące stowarzyszenie handlowe lub jednostki CCTV) zechciały je przyjąć poprzez przeprowadzenie odpowiednich szkoleń dla pracowników. Technologie na rzecz zwiększania prywatności mogą, ale nie muszą być projektowane w oparciu o specyfikacje, na przykład, rządów zamawiających systemy informacyjne i komunikacyjne, które mogą wykorzystywać takie technologie. Projektanci technologii opierają się na zapotrzebowaniu rynkowym przemysłu i społeczeństwa na ich produkty pozwalające na zwiększenie prywatności, gdyż jak wykazano, wiele spośród zaawansowanych narzędzi służących do anonimizacji i szyfrowania okazało się nieskutecznych. Inne przykłady zestawu narzędzi podkreślające wzajemną zależność mogłyby również zostać wzięte pod uwagę. Problem polega na tym, że współdziałanie i konflikty występujące pomiędzy różnymi elementami nie zostały dokładnie zidentyfikowane czy rozpoznane w praktyce, tak więc ich potencjał jako metod regulowania ingerencji w prywatność oraz bardziej rozległe konsekwencje nadzoru nie zostały dogłębnie zbadane. Ponadto nie jest jeszcze jasne, kto, jeśli ktokolwiek, powinien ponosić odpowiedzialność za promowanie niezależnego stosowania tych instrumentów lub za lepsze zaprojektowanie ich współdziałania.

44.4. Drugi problem, który nawiązuje do ostatniego punktu, zgodnie z naszą opinią polega na tym, że jest coraz mniej dowodów na to, że kontrola ma miejsce wyłącznie lub głównie na poziomie każdej krajowej (lub innej, większej lub mniejszej) jurysdykcji. Dany naród-państwo stanowi główne pole działań nadzorujących uzasadnionych bardzo ważnymi powodami o charakterze politycznym, prawnym, gospodarczym, społecznym i kulturalnym. Obecność instrumentów i dokumentów międzynarodowych była odczuwana na poziomie krajowym w zakresie ustawodawstwa, niekiedy wdrażającego wymogi międzynarodowe, jak ma to miejsce w przypadku państw członkowskich Unii Europejskiej dokonujących transpozycji dyrektyw UE do przepisów krajowych. Czasami zdarza się, że zagraniczny wzór lub model krajowego podejścia ustawodawczego zostaje przejęty bez takiego przymusu, lecz w przypadku gdy dany kraj ma podobne doświadczenia i czerpie z wiedzy innych krajów³⁰⁴ lub gdy takie rozwiązania zostały na niego

³⁰⁴ Bennett, C. (1997) 'Understanding ripple effects: The cross-national adoption of policy instruments for bureaucratic accountability [Zrozumienie efektu odbicia: Transnarodowe przyjęcie instrumentów polityki zapewniających odpowiedzialność biurokratyczną]'. *Governance* 10 (3): 213-33

nałożone działaniami innych krajów lub grup: porozumienie „Bezpieczna przystań” zawarte pomiędzy USA a UE jest tego przykładem.

- 44.5. W zasadzie kraje nie musiały wynaleźć przysłowiowego koła; istniejące przepisy prawne i doświadczenie wykraczające poza granice krajowe lub jurysdykcyjne zostały wykorzystane lub zignorowane jako światowe źródło wiedzy. Bez względu na to, ustanawianie przepisów prawnych odbywa się lub może się odbywać na różnych poziomach i pomiędzy nimi lub na krzyżujących się płaszczyznach począwszy od lokalnej po globalną oraz w różnych sektorach (np. telekomunikacji, handlu, transporcie, usługach publicznych) przy uwzględnieniu różnych instrumentów prawnych. Na przykład, pozostawiając bez komentarza skuteczność zastosowanych mechanizmów regulacyjnych, niektóre praktyki w zakresie nadzorowania miejsca pracy mogą być uregulowane na poziomie przedsiębiorstwa, wówczas mają zastosowanie kodeksy praktyk; jednakże mogą one zostać określone na poziomie kraju, w którym znajduje się dane przedsiębiorstwo, o ile istnieją ustawy lub nadrzędne kodeksy regulujące czynności realizowane w miejscu pracy; a także na poziomie globalnym, gdzie obowiązuje kodeks praktyk w zakresie prywatności pracownika³⁰⁵ ustanowiony przez Międzynarodową Organizację Pracy.
- 44.6. Patrząc na problem z drugiej strony, UE nie jest jedynym regionalnym lub globalnym podmiotem funkcjonującym jako źródło lub miejsce działań regulacyjnych dla niektórych krajów: kraje obszaru Azji i Pacyfiku opracowały ostatnio Politykę Prywatności, która jednakże spotkała się z krytyką, gdyż uznano, że reprezentuje niski standard³⁰⁶. Innym międzynarodowym podmiotem o potencjalnej mocy prawodawczej w zakresie objętego nadzorem globalnego przepływu informacji i przetwarzania danych osobowych jest Światowa Organizacja Handlu. Próba opracowania standardów prywatności, które mają być stosowane na całym świecie jest trudnym i politycznie nacechowanym procesem, jednakże odzwierciedla ona sposób, w jaki odbywają się działania poza granicami poszczególnych państw, potencjalnie wpływając na nie i na organizacje prowadzące działalność w tych państwach, a także na ich społeczeństwa. Standaryzacja lub ochrona prywatności, poza tą związaną z bezpieczeństwem technicznym systemów informacji oraz procedurami oceny zgodności w organizacjach, została uznana przed wiele stron za ważny krok w procesie prawodawczym, chociaż jej zasady nie zdobyły szczególnego uznania na ważnych arenach politycznych.
- 44.7. Kolejnego zestawu przykładów międzynarodowej ochrony danych i procedur prawodawczych w zakresie nadzoru na poziomie regionalnym mogą dostarczyć instytucje UE i inne instytucje europejskie. Grupa robocza Art. 29, w której skład wchodzi rzecznicy państw członkowskich, jest godnym uwagi organem ze względu na ilość i zakres wydanych sprawozdań, opinii, dokumentów roboczych i innych dokumentów od 1997 r. na wiele tematów obejmujących stosowanie biometrii, monitoringu, przekazywanie danych o pasażerach (PNR) z UE do USA, nadzór w miejscu pracy, dane genetyczne, technologię RFID i wiele innych, których łączna suma przekracza 100.³⁰⁷ Ustanowienie roli Europejskiego Inspektora Ochrony Danych (EDPS),³⁰⁸ do którego zadań należy monitorowanie przy zastosowaniu ICT oraz innych technologii, doradztwo i wywieranie wpływu na politykę Wspólnoty

³⁰⁵ International Labour Organization (ILO) (1997) „*Protection of Workers' Personal Data: An ILO Code of Practice [Ochrona danych osobowych pracowników: Kodeks Praktyki ILO]*”. Geneva: ILO.

³⁰⁶ Greenleaf, G. (2005) „APEC's Privacy Framework: a new low standard [Struktura Ramowa Prywatności APEC: nowy niski standard]”. *Privacy Law & Policy Reporter* 11: 121-4.

³⁰⁷ Zob. CEC Dyrekcja Generalna Wymiaru Sprawiedliwości i Spraw Wewnętrznych (bd.) „Grupa robocza Art. 29 ds. ochrony danych”, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

³⁰⁸ Zob. EDPS (bd.) „Introduction [Wprowadzenie]”, http://www.edps.europa.eu/01_en_presentation.htm; EDPS (bd.) „Duties of the European Data Protection Supervisor and Deputy Supervisor [obowiązki europejskiego inspektora ochrony danych i jego zastępcy]” roz. 5.4, http://www.edps.europa.eu/01_en_sub_fonctions.htm#Chap_54

Europejskiej w zakresie ochrony danych osobowych oraz rozwój sieci globalnych i istniejących na niższych poziomach, odbywanie spotkań i rozmów z rzecznikami w zakresie ważnych kwestii dotyczących prywatności i technologii, jest jednym ze sposobów na zapewnienie, że działania w zakresie prawodawstwa będą miały charakter transgraniczny. Inne organy międzynarodowe lub europejskie, takie jak Eurojust³⁰⁹ pomagający w dochodzeniu i ściganiu poważnych przypadków zorganizowanej przestępczości transgranicznej, posiadają własnych urzędników odpowiedzialnych za ochronę danych oraz odpowiednie zasady w zakresie ochrony danych osobowych.

44.8. Jednakże szacunkowa ocena wydajności tych poziomów pracy w zapobieganiu bardziej podstawnym formom nadzoru i ingerencji w prywatność oraz w naprawie ich skutków może być przedmiotem dyskusji, zwłaszcza przy obecnie panującym nieprzychylnym nastawieniu do opinii, że działania w zakresie zwalczania terroryzmu oraz egzekwowanie prawa mają pierwszeństwo przed wartościami związanymi z prywatnością oraz ograniczaniem nadzoru. Ponadto istnieje dużo luk charakterystycznych dla organizacji dotyczących określenia ról, instytucji, zakresu odpowiedzialności i strategii ochrony przed nadzorem. Poza tym to, czy możliwa jest koordynacja procedur prawodawczych pomiędzy krajami i różnymi poziomami oraz wykorzystywanie ustalonych opinii w celu skutecznego wywarcia wpływu na arenie rządowej i światowej, na których tworzy się autorytatywne polityki i podejmuje decyzje, również nie jest pewne. W UE, krajowe organy nadzorcze w zakresie ochrony prywatności otrzymały nakaz współpracy w niektórych dziedzinach. Ponadto w UE istnieje zespół globalnych i europejskich sieci wymiany informacji podejmujących badania w zakresie niektórych zagadnień i problemów dzięki czemu prawodawcy mogą być lepiej informowani, bardziej skuteczni i lepiej koordynować swoje zadania. Jednakże złożone problemy i sytuacje polityczne w dużym stopniu wpływają na losy tych lub innych form działalności prawodawczej, chociaż nie przekreślają ich.

44.9. Trzecim głównym problemem jest to, że przepisy prawne dotyczące nadzoru, w tym ochrony danych i prywatności nie dotrzymują kroku zaawansowanym technologiom, praktykom i celom nadzoru. Ani zasady dotyczące ochrony danych, ani niekompletny stan instrumentów regulacyjnych nie wydają się w pełni odpowiadać wyzwaniom, jakie w przyszłości prawdopodobnie mogą pojawić się z prywatnych, publicznych i mieszanych źródeł. Pojawienie się wielu nowych technologii informacyjnych i komunikacyjnych (ICT), w tym Internetu i technologii mobilnej, oraz powstające środowisko AmI i wszechobecna komputeryzacja integrująca liczne i zróżnicowane urządzenia nadzorujące stawiają pod znakiem zapytania skuteczność koncepcji i instrumentów regulacyjnych, na podstawie których zapoczątkowano rozwiązywanie różnych problemów przy wykorzystaniu scentralizowanego komputera lub nawet laptopa, telefonu komórkowego i Internetu. W niniejszym raporcie w dyskusji poświęconej telekomunikacji w Zjednoczonym Królestwie pojawiło się pytanie, czy nakładanie się kompetencji różnych krajowych organów prawodawczych, nieporozumienia dotyczące odpowiedzialności i różniące się interpretacje kluczowych pojęć i terminów dodatkowo utrudniają proces prawodawstwa. Ponadto globalny charakter procedur telekomunikacyjnych sprawia, że przydział zadań w zakresie prawodawstwa na poziomie krajowym i międzynarodowym jest sprawą niecierpiącą zwłoki, jeżeli problemy związane z niepewnością i słabą kontrolą mają być rozwiązane.

³⁰⁹ Zob. Eurojust (bd.) <http://www.eurojust.eu.int> ; EDPS (bd.) „Data Protection Officers appointed by the Community institutions and bodies [Urzednicy ochrony danych mianowani przez instytucje i organy wspólnotowe]”, http://www.edps.europa.eu/05_en_reseau_dpo.htm

- 44.10. Problemy i perspektywy w zakresie prawodawstwa pojawiające się w świecie chipów RFID, urządzeń do wykrywania, monitorowania i śledzenia, biometrii i innych technologii, które będą coraz częściej wykorzystywane w miejscu pracy i w środowisku domowym, a także w podróży i w rozrywce są zniechęcające. Prywatność w Internecie,³¹⁰ kiedyś uważana za najnowszą technologię w badaniu prywatności, nie jest jednakże szczytem osiągnięć, jeśli chodzi o możliwości regulacji projektowania i wykorzystywania technologii informacyjnej wykorzystywanej w przetwarzaniu danych. Ponadto procedury internetowe i Aml wchodzą ze sobą w interakcje, zacierając istniejące pomiędzy nimi różnice jako procedurami realizowanymi „online” i „offline”, „ręcznie” i „komputerowo”, „w sektorze publicznym” i „prywatnym” i nie są już skomplikowanymi działaniami binarnymi stosowanymi w celach regulacyjnych. Kodeksy praktyki mogą nie mieć tu żadnego znaczenia i zostać z łatwością pominięte, nawet jeśli istnieją. Dawne procedury powiadamiania, dokonywania wyboru, opowiadania się za lub przeciw, określenia preferencji dotyczących prywatności, oświadczenia dotyczące polityki prywatności, znaki prywatności i inne podobne procedury mogą jutro stać się nieważne w świecie płynności informacyjnej. Bez względu na to, czy powyższe okaże się być prawdziwe, to, jak powinien wyglądać podział odpowiedzialności oraz na czyich barkach powinna ona spoczywać w celu zwiększenia świadomości konsumentów i obywateli oraz zdolność oceny ryzyka, środki ochrony, przepisy prawne i środki zaradcze pozostaną prawdopodobnie ważnymi pytaniami w środowisku nowego nadzoru. Podobnie jest z pytaniem o to, w jaki sposób można chronić prywatność osób posiadających mniejsze zdolności w nauce lub pozbawionych możliwości technologicznych; należy zauważyć, że te osoby nie stanowią marginalnej mniejszości.
- 44.11. Generalnie nie są to całkowicie nowe problemy: wygląda na to, że każda nowa generacja technologiczna zdaje się powodować, że uprzednio obowiązująca polityka prawodawcza staje się całkowicie lub częściowo zbędna. W pewnym stopniu zostało to przewidziane, poprzez na przykład, brak nawiązań w ustawie do jakiegokolwiek konkretnej technologii, jak technologia komputerowa, dzięki czemu pozostaje ona aktualna w przypadku zmiany technologii. Jednakże od pojawienia i rozprzestrzenienia się Internetu zbieżność technologii i interakcja praktyk informacyjnych typu online i offline, a także elastyczność systemów prawodawczych przechodzi ciężką próbę. Jeżeli gromadzenie informacji i ich dalsze przetwarzanie, w tym przekazywanie, będzie wkrótce wszechobecne, zarówno zdolność instrumentów prawnych, nawet jeśli one współdziałają ze sobą wzajemnie, jak i poziomów i obszarów jurysdykcyjnych, nawet jeśli byłyby lepiej zintegrowane i uzasadnione, będzie nieodpowiednia z wielu powodów, chociaż nadal będzie bardzo odpowiednia do zapewnienia kontroli tego rodzaju praktyk nadzoru, jakie są już znane.
- 44.12. Ponadto, jeśli chodzi o rozwinięte systemy prawodawcze, zostały one zaprojektowane głównie w celu zapewnienia kontroli prywatności informacji w rozumieniu powszechnym; wątpliwości dotyczą również ich możliwości radzenia sobie rozszerzeniem nadzoru na inne dziedziny, w których dany organ, wykorzystanie przestrzeni i inne aspekty prywatności zostają objęte, jak to się dzieje z wieloma nowymi technologiami, „nowym nadzorem”. Najbardziej spójny i najdokładniej zaplanowany zestaw zasad i technik dotyczy ochrony danych osobowych, a nie przemieszczeń, obecności fizycznej w określonych rodzajach miejsc lub nietykalności cielesnej jako takiej, chociaż są one również związane z

³¹⁰ Raab, C. (2006) „The safe online consumer: Addressing issues and problems [Konsument bezpieczny w sieci: Omówienie problemów i zagadnień]”, Praca przedstawiona na 56 Dorocznej Konferencji International Communication Association, Drezno, 19-23 czerwca, panel poświęcony *Indywidualnym i społecznym perspektywom bezpieczeństwa w sieci*; Lace (ed.) (2005) *op cit.*, nr 6.

przetwarzaniem informacji i danych osobowych, dlatego też w pewnym stopniu podlegają odpowiednim przepisom prawnym. Jednakże należałoby się wykazać niezwykłą pomysłowością, aby objąć nadzorem te rodzaje ludzkiego zachowania oraz kontrolować je przepisami prawnymi i założeniami ustanowionymi w przeszłości, czego dowodzą liczne sprawy sądowe. Rozwiązanie alternatywne – ustanowienie nowych praw dla każdej nowej technologii – utrzymałoby tylko niespójny charakter wielu przepisów dotyczących prywatności, stwarzając stale rozprzestrzeniający się oszalałający gąszcz specjalnych przepisów, które mogą działać wbrew tendencji do upraszczania, ujednolicania i uogólniania kontroli. Wszechstronne przepisy i pełniące wiele funkcji organy ochrony danych nie wykazują już tendencji uogólniania i przewyższyły również taki sposób myślenia, zgodnie z którym raz ustanowione sektory publiczne i prywatne stanowią według prawa oddzielne obszary, podczas gdy świat i przepływ danych zmierzają w przeciwnym kierunku. Wspomniane niektóre przepisy sektorowe oraz kodeksy praktyki są użyteczne w połączeniu z metodami ogólnymi, a niektóre z nich są związane z konkretnymi praktykami technologicznymi, takimi jak telekomunikacja i monitoring. Mimo to niełatwo jest przewidzieć, w jaki sposób rodzina taka jak Jonesowie mogłaby zastosować środki samopomocy wobec wszechobecnego i często ukradkowego nadzoru, z jakim mają do czynienia na co dzień.

- 44.13. Te trzy grupy problemów mogą nie być jedynymi, jakich należy się spodziewać, jednakże są wystarczające do podsumowania wielu już istniejących i potencjalnych wad przepisów prawnych określających wyzwania, jakim należy sprostać, aby możliwe było kontrolowanie nadzoru i złagodzenie jego skutków ubocznych, jakie wywiera na całą gamę wartości bliskich człowiekowi.

45. Możliwości rozwoju prawodawstwa

45.1. Ocena wpływu na prywatność

- 45.1.1. Uważamy, że istotne korzyści mogłoby przynieść przyjęcie metody oceny wpływu na prywatność (PIA) w praktykach prawodawczych jurysdykcji na wszelkich poziomach, na których jest to konieczne.³¹¹ PIA może być postrzegana jako instrument, z którego mogą korzystać ci, którzy proponują wdrożenie nowych lub rewizję starych systemów informacji przetwarzających dane osobowe w celu złagodzenia potencjalnych szkodliwych skutków, jakie te systemy mogą wywierać na prywatność osób, których przetwarzane dane dotyczą. Rozważmy istniejącą teorię i praktykę PIA, pomijając jej ewentualne wady i ograniczenia.

45.1.2. W uproszczeniu PIA może być postrzegana jako:

- „ocena wszelkiego rzeczywistego lub potencjalnego wpływu, jaki dane działania lub propozycje mogą wywierać na prywatność poszczególnych osób oraz sposobów, jakie mogą posłużyć do złagodzenia wszelkich niepożądanych skutków”³¹²;

³¹¹ Stewart, B. (1999) „Privacy impact assessment: towards a better informed process for evaluating privacy issues arising from new technologies [Ocena oddziaływania na prywatność: działania na rzecz bardziej świadomego procesu oceny zagadnień dotyczących prywatności w kontekście nowych technologii]”, *Privacy Law & Policy Reporter* 5 (8): 147-149; rozważania nad PIA są dostępne w pracy Raab, C., 6, P., Birch, A. i Copping, M. (2004) „*Information Sharing for Children at Risk: Impacts on Privacy*”, [Wymiana informacji i zagrożenia dla dzieci: Oddziaływanie na prywatność], Edinburgh: Scottish Executive.

³¹² Stewart, B. (1996) „Privacy impact assessments [Ocena oddziaływania na prywatność]”, *Privacy Law & Policy Reporter* 3 (4): 61-4.

- „proces. Fakt przechodzenia przez ten proces i badanie poszczególnych opcji wskaże szereg alternatyw, które w przeciwnym razie mogłyby zostać pominięte”;³¹³
- podejście i filozofia, które zapowiadają zakorzenienie skuteczniejszej kultury zrozumienia i praktyki w organizacjach przetwarzających dane osobowe;
- forma oceny ryzyka, która nie jest wolna od niepewności przy identyfikacji i ocenie powagi i prawdopodobieństwa wystąpienia różnego rodzaju zagrożeń, które mogą dotyczyć prywatności, życiowych szans, dyskryminacji, równości itd.
- narzędzie pozwalające na rozwinięcie proponowanych technologii lub aplikacji w kierunku dogłębnej analizy, debaty i działań zapobiegawczych w ramach zainteresowanych organizacji;
- jak w przypadku PET, opiera się na założeniu, że zabezpieczenia powinny być wbudowane, nie zaś nabudowane;
- technika wczesnego ostrzegania skierowana do polityków i operatorów systemów przetwarzania danych osobowych, pozwalająca im na zrozumienie i rozwiązanie konfliktów zachodzących pomiędzy ich celami i praktykami a wymaganą ochroną prywatności wykraczającą poza kontrolę nadzoru;
- najlepiej jako dokument publiczny pozwalający na zwiększenie przejrzystości oraz zwiększenie świadomości społeczeństwa w zakresie problemów i zagrożeń związanych z nadzorem; to, z kolei, może wesprzeć organy prawodawcze w zakresie skuteczniejszej realizacji ich obowiązków.

45.1.3. Dlatego też korzystny jest nie tylko raport będący wynikiem PIA, ale również sam proces oceny. Technika ta jest zalecana w USA i w Kanadzie dla nowych projektów realizowanych w ramach sektora publicznego w zakresie przetwarzania danych osobowych, jakie mają miejsce na szczeblu federalnym. W Zjednoczonym Królestwie pojawiły się opinie wzywające do stosowania PIA w odniesieniu do konkretnych projektów np. dotyczących dowodów tożsamości. Wydział Wykonania Zadań³¹⁴ i Innowacji rozważał tą możliwość w kontekście wymiany danych w brytyjskim sektorze publicznym a Narodowa Rada Konsumentów³¹⁵ zaleciła stosowanie oceny rządowi i firmom wzywając jednocześnie do zmiany Ustawy o ochronie danych z 1998 r., która miałaby wprowadzać taki wymóg, a także Rzecznika ds. Informacji do zaangażowania się w sprawę. W Szkocji przeprowadzono studium wykonalności w zakresie stosowania PIA w rządowych planach dotyczących systemu informacji w zakresie opieki społecznej.³¹⁶ Jednakże istnieje pewien opór wobec rozwijania i wprowadzania wymogu stosowania jawnego instrumentu oceny w instytucjach publicznych, nawet jeśli zapewnienia rządu dotyczące poważnego podejścia do prywatności w jego długoterminowych planach dotyczących e-government i informatyzacji służb publicznych nawiązują w pewien sposób do PIA, to nawiązanie to nie jest wyraźne.

³¹³ Stewart, B. (1996) „PIAs – an early warning system [PIA jako system wczesnego ostrzegania]”. *Privacy Law & Policy Reporter* 3 (7): 134-8.

³¹⁴ Performance and Innovation Unit (PIU), Cabinet Office (2002) „*Privacy and Data-Sharing: The Way Forward for Public Services [Prywatność a wymiana informacji: Rozwój służb publicznych]*”. London: Cabinet Office.

³¹⁵ Lace, S. (2005) „The new personal information agenda [Nowa agenda danych osobowych]”, Lace (ed.) *op cit.* nr 6: 217-9.

³¹⁶ Raab, C. *et al.*, *op cit.* nr 310.

45.1.4. Istnieje wiele zróżnicowanych modeli wdrażania³¹⁷, jednakże nie mogą one zostać opisane w niniejszym opracowaniu. Procedury stosowania PIA wymagają, aby osoby wdrażające inicjatywy dokładnie zrozumiały procedurę przepływu danych, jaka ma miejsce w ich systemach oraz rozwiązywały kwestie wykraczające poza zwykłą zgodność prawną, chociaż pewna wersja zestawu zasad omówiona powyżej jest zazwyczaj stosowana jako podstawa. PIA nie powinna być mylona w audytami zgodności i podobnymi kontrolami, które są zazwyczaj przeprowadzane retrospektywnie i są ukierunkowane na kontrolowanie zgodności prawnej. Podobnie jak ocena wpływu na środowisko PIA ocenia prawdopodobne oddziaływanie aplikacji lub nowych systemów w przyszłości i stosuje szersze kryteria. Od lat 1990. Obserwuje się rozwój literatury praktycznej w dużej mierze związanej z dążeniami niektórych organów prawodawczych właściwych w zakresie prywatności i ochrony danych w kierunku opracowania i wdrożenia lub zachęcania do przyjęcia oceny PIA jako instrumentu zapobiegawczego do oceny prawdopodobnego wpływu na prywatność, jaki wywierają nowe technologie lub proponowane systemy i praktyki w zakresie przetwarzania informacji.³¹⁸ Z jednej strony uważa się, że PIA mogłaby zmniejszyć obciążenie spoczywające na urzędnikach ustanawiających przepisy prawnych związane z zapewnieniem zgodności co najmniej działań administratorów danych z ustawami i zasadami oraz obsługą skarg osób których dane dotyczą, poprzez jej wkład w projektowanie technologii i praktyk w taki sposób, aby zredukować ich negatywny wpływ na prywatność.

45.1.5. Systemy informacji i nowe metody pracy stosowane w różnych organach są często wdrażane bez odpowiedniego zrozumienia wymogów dotyczących prywatności lub i innych związanych z tym konsekwencji. Jeżeli odpowiednie zabezpieczenia nie zostaną pierwotnie wbudowane w procedurę przetwarzania danych, operatorzy będą musieli je dodać, co nie zawsze jest możliwe bez odwoływania się do kosztownych i kłopotliwych forteli, które mogą szkodzić funkcjonowaniu systemu. W odniesieniu do polityków wyższego szczebla PIA pomaga zapewnić, że systemy informacyjne ustanowione w procesie wdrażania polityk łagodziły zagrożenia (co najmniej) lub zwiększały korzyści (co najwyżej). PIA pomaga obywatelom ograniczać stopień, w jakim odwołują się oni do skarg i korzystania ze środków zaradczych w przypadku naruszenia wymogów dotyczących ochrony danych lub praw człowieka. Dlatego też rola PIA może polegać na zapewnianiu obywateli o tym, że przetwarzanie ich danych lub inne praktyki w zakresie nadzoru są dobrze chronione lub zminimalizowane. W związku z tym PIA pomaga w utrzymaniu lub tworzeniu zaufania.

³¹⁷ Jako przykład mogą posłużyć: Biuro rzecznika ds. informacji i prywatności Alberta (2001) „*Privacy Impact Assessment [Ocena oddziaływania na prywatność]*”: Rząd Kolumbii Brytyjskiej, Ministerstwo Usług Rządowych; Rząd Kolumbii Brytyjskiej, Ministerstwo Usług Rządowych (2003) „*Privacy Impact Assessment (PIA) Process [Procedura oceny oddziaływania na prywatność]*”. Victoria: Biuro ds. informacji i prywatności, Ontario (2001) *Privacy Impact Assessment - A User's Guide [Ocena oddziaływania na prywatność – Podręcznik użytkownika]*. Toronto ON: Sekretariat administracji, Biuro ds. informacji i prywatności, Ontario; Biuro rzecznika ds. prywatności, Nowa Zelandia (2002) „*Guidance Notes: Privacy Impact Assessment Handbook [Wtyczne: Podręcznik oceny oddziaływania na prywatność]*” Auckland: Biuro rzecznika ds. prywatności, Nowa Zelandia; Sekretariat Rady Skarbu, Kanada (2002) „*Privacy Impact Assessment Guidelines: A Framework to Manage Privacy Risks [Wtyczne dotyczące oceny oddziaływania na prywatność: Struktura ramowa zarządzania ryzykiem związanym z prywatnością]*”, wersja 2.0, z dnia 31 sierpnia. Ottawa, ON: Sekretariat Rady Skarbu, Kanada; Ministerstwo Spraw Wewnętrznych, Stany Zjednoczone, Biuro dyrektora ds. informatyki (2002) „*Department of the Interior Privacy Impact Assessment and Guide [Ministerstwo Spraw Wewnętrznych, Ocena oddziaływania na prywatność, Wtyczne]*”, wersja: 9.16.02. Waszyngton: Ministerstwo Spraw Wewnętrznych, Stany Zjednoczone, Biuro dyrektora ds. informatyki.

³¹⁸ Użyteczne informacje można znaleźć w Clarke, R. (bd.) „*Privacy Impact Assessments [Ocena wpływu na prywatność]*” <http://www.anu.edu.au/people/Roger.Clarke/DV/PIA.html>. Zob. również: Waters, N. (2001) „Privacy impact assessment – traps for the unwary [Ocena wpływu na prywatność – pułapki czyhające na nieostrożnych]”, *Privacy Law & Policy Reporter* 7 (9): 176-7; White, F. (2001) „The use of privacy impact assessments in Canada [Zastosowanie oceny oddziaływania na prywatność w Kanadzie]”, *Privacy Files* 4: (7/8).

45.1.6. Obserwuje się znaczące polityczne i administracyjne dążenie do wprowadzenia nadzoru, gdzie prywatność, poufność i prawa człowieka są postrzegane często jako przeszkoda lub ograniczenie, które w „bilansie” powinny zostać oszacowane jako mniejszej wartości. PIA może pomóc w wykazaniu, w jaki sposób ochrona prywatności może zostać wprowadzona do mechanizmu wymiany informacji jako ważny wymóg etyczno-prawny, który może przyczynić się na rzecz osiągnięcia ważnych celów społecznych i politycznych takich, jak lepsze, w większym stopniu zorientowane na obywatela służby publiczne lub bezpieczeństwo, nie zaś jako przeszkoda w ich osiągnięciu.

45.1.7. Możemy podsumować i kontynuować dyskusję poprzez określenie tego, czym PIA nie jest. PIA nie jest:

- zwykłym narzędziem służącym do zapewnienia zgodności: jej zwolennicy widzą w niej sposób na usprawnienie praktyki wykraczające ponad minimum niezbędne do spełnienia wymogów prawnych;
- mechanizmem audytu: ocenia oddziaływanie nowych i proponowanych systemów, najlepiej tuż przed ich wdrożeniem;
- w większości jurysdykcji, prawnie wiążącym lub ostatecznym dokumentem: jej wpływ może być istotny lub przekonujący, a w niektórych miejscach (jak USA czy Kanada) wymóg dotyczący przeprowadzania PIA ma już charakter prawny;
- nałożona z zewnątrz: najlepiej, aby była przeprowadzana i „należała” do interesariuszy danej organizacji;
- przeznaczona do oceny wszystkich procedur jednocześnie: podlega rewizji w miarę zmian zachodzących w systemach i zmian okoliczności;
- sposobem do zatrzymania procesu przetwarzania danych: jej celem jest ułatwienie tego procesu poprzez analizę ryzyka dotyczącego prywatności lub nadzoru oraz ich eliminacja lub łagodzenie;
- przede wszystkim sposobem oceny zagrożeń przed jakimi stoi dana *organizacja*: jej głównym celem jest zredukowanie zagrożeń dotyczących osoby, której dotyczą dane, chociaż zagrożenia odnoszące się do organizacji też są uwzględniane;
- uniwersalnym szablonem: istnieją jednakże pewne wzory; PIA powinna być dostosowana tak, aby oceniać procedury informacyjne konkretnej organizacji;
- testem wyboru dającym na końcu konkretną odpowiedź lub wynik: jest sposobem pozwalającym na stawianie pytań, na które trzeba udzielić odpowiedzi i wskazanie problemów, które muszą zostać rozwiązane.

45.1.8. Ponadto nie jest ona cudownym lekiem, który można wprowadzić do operacji przedsiębiorstwa lub państwa niewymagającym nakładów finansowych ani zmian w praktyce pracy, chociaż uniknięcie kosztownych pomyłek oraz osiągnięcia w zakresie polityki, reputacji i wiarygodności powinny wyrównywać poniesione nakłady. Wdrożenie PIA może nie być proste, czy też obiecywać łatwych rozwiązań dotyczących problemów związanych z decyzjami dotyczącymi wdrażania nadzoru. Powszechnymi błędami są powierzchowne, zorientowane na zachowanie zgodności i niezobowiązujące podejście do wyników badania; poczucie odłączenia od procesu, zwłaszcza jeżeli PIA nie jest przeprowadzana i inicjowana przez zainteresowaną organizację; oraz brak powiązania pomiędzy procedurą PIA, jej wynikami i najważniejszymi decyzjami. Najlepiej PIA powinna dotyczyć systemu informacji lub aplikacji

technologicznej, odpowiadając na pytania: dlaczego one istnieją i w jaki sposób gromadzą, wykorzystują, udostępniają i przechowują informacje osobowe. W tym procesie konkretne problemy dotyczące prywatności pojawiają się i mogą zostać rozwiązane w zrozumiały sposób na podstawie rozważnych przemyśleń i dokładnych informacji.³¹⁹

45.1.9. Z drugiej strony upewnienie się co do wszystkich wymagań dotyczących systemu może okazać się trudne, a ocena ryzyka stanowiąca trzon PIA nie może być rzeczą prostą. Ryzyko może okazać się trudne lub niemożliwe do oszacowania, chociaż PIA nakłada na osoby zaangażowane obowiązek przeprowadzenia badań publicznych, dyskusji i być może debaty nad problemem ryzyka, niż raczej przyjęcia zwykłego rozumienia tego problemu. W ten sposób PIA promuje uzasadnione podejście do związku zachodzącego pomiędzy prywatnością a innymi, często przeciwstawnymi priorytetami. Dzięki temu PIA może wzmocnić przejrzystość i odpowiedzialność. PIA nie jest procedurą rozwiązującą wszelkie problemy: jej wynik ma na celu umożliwienie aktualizacji w miarę wprowadzania zmian w systemie, co niewątpliwie ma miejsce. Jeżeli rozważamy metodę PIA w kategoriach połączonej współpracy różnych organizacji i wymiany informacji, wówczas trudności mogą narastać. Jednakże systematyczne udzielanie odpowiedzi na pytania stawiane przez PIA może stanowić strategiczny punkt wkroczenia w obszar zagadnień dotyczących ochrony informacji, kierownictwa, ról, protokołów itd., które zostały już uznane za bardzo ważne dla dobrej praktyki w ramach organizacji i pomiędzy nimi.

45.2. *Od oceny wpływu na prywatność po ocenę skutków nadzoru?*

45.2.1. Aby ująć potencjalnie szkodliwe skutki nadzoru w szerszym ujęciu niż ochrona prywatności, należałoby opracować narzędzia PIA wykraczające poza ich aktualną konfigurację oraz stworzyć narzędzie, które mogłoby się nazywać *ocena skutków nadzoru* lub SIA. To oczywiście wiąże się ze zmianą znaczenia, gdyż o ile PIA ocenia wpływ przetwarzania informacji na prywatność, SIA oznaczałaby ocenę wpływu nadzoru na zakres wartości, które mogą obejmować, ale nie tylko prywatność.

45.2.2. Trzeba przyznać, że jest to istotny minus, ale jednocześnie szansa dalszego rozwoju. W tym miejscu wracamy do naszych wcześniejszych uwag dotyczących ochrony prywatności i jej związku z ochroną przed nadzorem. Ze względu na to, że PIA została zaprojektowana jako narzędzie dotyczące prywatności, rozumianej w odniesieniu do praw osób fizycznych, nie jest ona najlepszą płaszczyzną do rozważań nad dalszymi konsekwencjami nadzoru w kategoriach innych różnych wpływów społecznych i osobistych. Aby było to możliwe, musiałaby nastąpić zmiana modelu oznaczająca odejście od rozpatrywania wyłącznie skutków dotyczących osoby fizycznej, jak ma to miejsce w przypadku rozważań nad prywatnością, na rzecz rozważań nad wartością ochrony prywatności i ograniczeniami nadzoru również w kategoriach społecznych.³²⁰ Prywatność nie stanowi wyłącznie indywidualnej wartości, ale jest również ważna z punktu widzenia społeczeństwa jako podstawa wspólnego dobra oraz wspólnych wartości takich jak demokracja, zaufanie, umiejętność życia w społeczeństwie oraz wolne i równe społeczeństwo. Ma to swoje odzwierciedlenie w podejściu stosowanym przez

³¹⁹ Flaherty, D. (2004) „Privacy impact assessments (PIAs): An essential tool for data protection” [Ocena oddziaływania na prywatność: Podstawowe narzędzie ochrony danych]” Praca przedstawiona na 17 dorocznej konferencji Privacy Laws & Business, Cambridge, dnia 5-7 lipca, 2.

³²⁰ Regan (1995) *op cit.* nr 14, roz. 8.

właściwe organy prawodawcze, postępowe firmy i obrońców prywatności. Ze względu na to, że wartość prywatności wykracza poza daną jednostkę, wszyscy mamy interes w tym, aby każda osoba miała prawo i zdolność ochrony swojej prywatności dowolnymi instrumentami. Zarówno prywatność, jak i ochrona prywatności mają duże znaczenie dla społeczeństwa, obejmując jednocześnie kwestie wspólne, prywatne i zbiorowe. Stanowiąc wartość indywidualną i jedno z praw człowieka, prywatność jest również wartością powszechną, ponieważ wspólnym dobrem wszystkich osób jest prawo do prywatności, nawet jeśli zachodzą pomiędzy nimi rozbieżności co do elementów ich prywatności lub tego co uznają za szczególnie chronione. Jest to wartość publiczna, ponieważ stanowi trwałą podstawę społeczeństwa demokratycznego. Jest wartością zbiorą, ponieważ pod pewnymi względami i wraz z pewnymi instrumentami prawnymi stanowi wspólne dobro, które nie może zostać oddzielone od ochrony, której osoby fizyczne nie mogą zostać pozbawione i które nie może być skutecznie zapewniona przez rynek.³²¹

45.2.3. Jeżeli jest tak w przypadku prywatności, jest tak również w przypadku nadzoru i dotyczących go przepisów prawnych, ponieważ wiele praktyk w ramach nadzoru ma bezpośredni wpływ na charakter społeczeństwa, w którym są realizowane. Dotyczy to podziału na kategorie, a zatem dyskryminacji (lub nadania szczególnych uprawnień), wykluczenia społecznego i innych skutków, które nadal wzbudzałyby niepokój, nawet jeśli nie chodziłoby o ingerencję w prywatność danej osoby. Uwzględnienie społecznej wartości prywatności byłoby korzystne z perspektywy PIA i przepisów prawnych dotyczących prywatności. Jednakże wzięcie pod uwagę skutków społecznych byłoby całkowitą przemianą w świecie ochrony prywatności, jej instrumentów i systemów. Być może nie istnieje wiele krajowych lub innych systemów ochrony prywatności, w przypadku których zwiększenie ich zasięgu i w szczególności roli uczestników procesu prawodawczego, można by uznać za zgodne z prawem lub możliwe z punktu widzenia polityki w celu uwzględnienia ich szerszych skutków, które są bardziej namacalne, jeżeli są rozważane w kontekście nadzoru. Głównym celem przepisów prawnych dotyczących nadzoru jest zapewnienie ochrony międzyludzkich wartości społecznych oprócz wartości, jaką jest prywatność danej osoby. Dlatego też SIA mogłaby odgrywać znaczącą rolę poprzez przyłączenie PIA, jednakże rozszerzenie jej o pewien zakres pytań skierowanych na ocenę oddziaływania nadzoru lub ingerencji w prywatność na społeczeństwo oraz na inne, niezwiązane z prywatnością interesy poszczególnych osób, kategorii i grup osób.

45.2.4. Istnieją precedensy zwiększenia zakresu w innych dziedzinach: ocena oddziaływania na środowisko stała się częścią porozumień rządowych, przy czym wcześniej jej rola ograniczała się do produkcji żywności, transportu, dostaw energii, budownictwa przemysłowego i mieszkaniowego. Wpływ polityki rządowej na mniejszości rasowe lub etniczne jest obecnie postrzegany jako problem, który powinien zostać wzięty pod uwagę. To, czym jest innowacja ICT, nowa baza danych lub nowy mechanizm audiowizualny służący do monitorowania przestrzeni publicznej lub prywatnych pasażerów handlowych dla autonomii i godności osobistej, solidarności społecznej lub kontekstu interakcji społecznych nie stanowi niewyobrażalnego pytania, które nie mogłoby zostać zinstytucjonalizowane w ramach szeregu praktyk i wymogów stosowanych przed wdrożeniem takich możliwości nadzoru.

³²¹ *ibid.*

- 45.2.5. Wcześniej nawiązaliśmy do pytania Marksa o etyczność nadzoru: pytania te mogą korzystanie wpłynąć na SIA poprzez rozwój PIA, dlatego też dołączamy je w tej sekcji raportu.
- 45.2.6. Pytania dostosowujące, takie jak te mające na celu ocenienie wpływu nadzoru zostają postawione w takiej dziedzinie, w której środki wykorzystywane w gromadzeniu, kontekst gromadzenia danych i wykorzystanie nadzoru zostają poddane ocenie pod względem ich wpływu na poszczególne osoby i społeczności przejawiającego się szkodami fizycznymi lub psychicznymi, niesprawiedliwą dystrybucji procedur, zaburzeniami równowagi władzy i innymi, w tym poprzez standardowe kryteria zgodności ochrony danych obejmujące świadomość, zgodę, zadośćuczynienie, sankcje, cele itd. Powyższy wykaz jest zakorzeniony w głównym stanowisku etycznym oraz w określonych ramach prawnych, które zostały już ustanowione w wyniku zastosowania międzynarodowych instrumentów i przepisów prawnych, które omówiliśmy powyżej. Dlatego też nie zachodzi konieczność tworzenia całkowicie nowych podstaw w celu przeprowadzenia SIA lub PIA. To, czy zachodzi potrzeba stworzenia nowych politycznych podstaw jest pytaniem, na które odpowiedzi powinny udzielić poszczególne państwa i inne podmioty, nie zaś niniejszy raport.
- 45.2.7. Nie możemy wskazać w niniejszym raporcie, w jaki sposób SIA byłaby stosowana w praktyce, jednakże niektóre z pytań Marksa mogą zostać podkreślone jako pytania, które byłyby zadawane w ramach oceny SIA oprócz pytań głównych, które są bardziej bezpośrednio związane z prywatnością, jako taką. Na przykład pytanie dotyczące szkód („czy technika powoduje nieuzasadnione szkody fizyczne lub psychologiczne” lub „straty”?) nawiązuje do konsekwencji dla dobrego samopoczucia, które niekoniecznie muszą dać się naprawić na podstawie przepisów dotyczących ochrony danych lub innych przepisów w sprawie ochrony prywatności. Pytania dotyczące beneficjentów („czy stosowanie takiej taktyki służy szeroko pojętym celom społecznym, celom przedmiotu nadzoru lub osobistym celom osobie gromadzącej dane?”) nie mają na celu kompromitować tych ostatnich, ale uzasadniać wyniki techniki nadzoru w taki sposób, aby osoba zadająca takie pytania wiedziała, w jakim kierunku zmierza to badanie. Zapytanie dotyczące konsekwencji braku działań („jeżeli środki są bardzo kosztowne, jakie mogą być konsekwencje zaniechania nadzoru”?) ma na celu ocenę konieczności wprowadzenia nadzoru, nie tylko jego wykonalności lub tego, czy jest on pożądany.
- 45.2.8. Są to tylko niektóre przykłady sposobu przeprowadzenia SIA. Oczywiście jest, że ocena ta powinna obejmować szerszy zakres zagadnień niż tylko te dotyczące zgodności prawnej lub nawet prywatności osobistej. Każda SIA podobnie jak PIA musiałaby zostać dostosowana do szczególnych cech stosowanych praktyk i technologii³²², chociaż wówczas powstałoby znaczne, podstawowe podobieństwo pomiędzy dwoma badaniami, który byłyby widoczne w praktyce, ponieważ występuje pomiędzy nimi wiele podobieństw oraz istnieją powszechne wymogi prawne lub etyczne, które również powinny zostać spełnione.
- 45.2.9. Jak już wspomnieliśmy wcześniej, jeśli chodzi o PIA jedną z zalet SIA jest pomoc jaką zapewnia organom regulacyjnym i poszczególnym obywatelom w zrozumieniu i kontrolowaniu praktyk nadzoru poprzez

³²² Krótka dyskusja poświęcona Aml, jest opisana w Raab, C. (2006) „Regulating ambient intelligence: The road to privacy impact assessment? [Regulacje w świecie inteligentnego otoczenia: Droga do oceny oddziaływania na prywatność?]” Praca przedstawiona na Międzynarodowej konferencji nt. Zabezpieczenia w świecie inteligentnego otoczenia (SWAMI), Bruksela, w dniach 21-22 marca.

zwiększenie ich przejrzystości i odpowiedzialności osób, które je wprowadzają. W rzeczywistości są to główne cele swobodnego dostępu do informacji (FOI), stanowiącego przedmiot wdrażania pewnej liczby organów prawodawczych lub rzeczników powołanych specjalnie w tym celu. Jeżeli przeprowadzanie SIA byłoby konieczne w przypadku firm i organizacji publicznych, jako podstawa do dalszej dyskusji oraz zatwierdzenia, wówczas odgrywałyby one pewną rolę w otwarciu nadzoru na kontrole i opinie publiczne. Ponadto, jak już zostało wspomniane przy omawianiu PIA, organizacje czerpią pewne korzyści ze zrozumienia swoich własnych praktyk oraz tego, w jaki sposób mogą je ulepszyć, aby były bardziej zgodne z prawem, kodeksami praktyki ograniczającej nadzór i/lub z obrazem integralności i zaufania, jaki stara się zbudować dana organizacja.

45.3. *Inne możliwości*

45.3.1. Jeżeli SIA czerpie z PIA, inne możliwości również zostają oparte na istniejących. W szczególności chodzi nam o to, w jaki sposób rzecznicy zajmujący się zagadnieniem prywatności oraz inne organy prawodawcze mogą rozszerzyć swoje role, o ile pozwalają na to ich systemy polityczne, w celu zapewnienia powszechniejszego wdrożenia przepisów prawnych regulujących nadzór. Nie istnieją gotowe przepisy na przewyżczenie wielu trudności, jakich doświadczyli rzecznicy w wielu krajach podczas wykonywania swoich obowiązków na podstawie istniejących przepisów prawnych na dowolnym poziomie jurysdykcyjnym i pomiędzy nimi. Ponadto istnieją konkretne problemy związane z pełnieniem takich funkcji, których być może nikt jeszcze nie doświadczył.

45.3.2. W odniesieniu do nowego nadzoru, lecz również uwzględniając konwencjonalne wyzwania, uważamy, że organy prawodawcze powinny mieć większe uprawnienia i więcej środków do dyspozycji, takich jak sankcje, które mogliby nakładać, większy wpływ na politykę rządu i plany biznesowe, powinni być obciążeni mniej uciążliwymi, rutynowymi wymogami i zapewniać lepsze informowanie społeczeństwa. Należy to traktować jako „listę życzeń”, wobec której sprzeciwiłoby się kilku członków środowiska prawodawczego, jednakże niniejszy raport nie może przedstawiać bardziej konkretnych zaleceń w formie listy zakupów nieposiadającej konkretnego adresata lub nie dotyczącej żadnej konkretnej sytuacji, gdyż byłyby one nierealne. Dlatego też możliwe jest wyszczególnienie kilku konkretnych usprawnień, które wydają się pożądane, a także w wielu przypadkach wykonalne lub co najmniej możliwe jest wskazanie gdzie środowisko i procedury prawodawcze mogą być odpowiednie. Takie usprawnienia i wskazówki dotyczą sześciu obszarów trudności, jakie zostały rozpoznane na początku Części D:

- Prawodawstwo reaktywne: organy regulacyjne były często zaskakiwane wykorzystaniem biznesowym lub rządowym ICT lub proponowanymi systemami, które stanowią potencjalne zagrożenie dla prywatności lub pozwalają na wprowadzenie niebezpiecznego nadzoru. Organy prawodawcze, niezależnie od tego czy tworzą je urzędnicy czy też członkowie społeczeństwa obywatelskiego zaangażowani w politykę prywatności i nadzoru, mogą zostać odsunięci od polityki i szczebli decyzyjnych, na których takie plany są opracowywane i wdrażane lub też mogą przedstawić je zbyt późno, aby miały one wpływ na podejmowane decyzje. PIA lub SIA mogą pomóc w promowaniu bardziej proaktywnego podejścia, ale jedynie w takim stopniu, w jakim polityki i

plany zostaną odpowiednio wcześniej udostępnione. W odniesieniu do organów regulacyjnych, dobrze byłoby, gdyby ich wczesne interwencje i kontrole były poparte wymogami statutowymi lub innymi. Jednakże zdolność do wkroczenia na arenę polityczną, w wielu przypadkach, może zostać porównana do zdolności organów prawodawczych do „bycia na bieżąco” i pozyskiwania wiedzy dotyczącej nowych technologii i systemów, dlatego też ich zdolność instytucjonalna może wymagać poprawy, co miałyby istotne konsekwencje. Konsekwencje te, z kolei, mogą powodować znaczne trudności na każdym poziomie jurysdykcyjnym. Dlatego też zaleca się, aby dalej rozwijać zdolności w zakresie posiadanej wiedzy technologicznej i świadomości, co może nastąpić, na przykład, na szczeblu UE, poprzez Grupę Roboczą Art. 29 i inne sieci i kanały łączące wiele krajowych i regionalnych organów prawodawczych.

- Przepisy techniczne i dotyczące zarządzania: takie strategie i instrumenty mogą częściowo zawierać antidotum na zbyt rozbudowane przepisy prawne, stanowiące drugi obszar trudności. Mogłyby być szczególnie pomocne w przewidywaniu, a także w przypadku przeprowadzania PIA i SIA, wspierać osoby przedstawiające propozycje dotyczące nadzoru w łagodzeniu niepożądanych skutków poprzez wprowadzenie zmian organizacyjnych, szkolenia pracowników, usprawnienia w zarządzaniu informacjami korzystne dla prywatności itd. Byłoby to pomocne we wprowadzaniu opartych na prawie metod regulacyjnych w szerszym kontekście strategii. Takie podejście może być już obecne w wielu systemach, chociaż w mniejszym stopniu na szczeblu międzynarodowym, tak więc wciąż wymaga wsparcia. Ponadto korzystne byłoby, jeżeli działania na rzecz rozwoju standardów w zakresie prywatności na poziomie międzynarodowym nabrały impetu. Standaryzacja uprościłaby obciążenia prawne nałożone na organy i przyczyniłaby się do wsparcia wysiłków organizacji w zakresie samoregulacji, a także w zapewnieniu działań na rzecz informowania opinii publicznej. Takie działanie może być szczególnie korzystne w kontekście nowych technologii i przetwarzania w oparciu o nie informacji. To wskazywałoby również na istnienie korzystnego współdziałania pomiędzy niektórymi wyżej wymienionymi instrumentami prawnymi.
- Pojęcie „prywatności”: pojęcie to zostało już przez nas omówione przy okazji wyjaśniania potrzeby szerszego spojrzenia, ogólnie mówiąc, na społeczną wartość prywatności, która jest przedmiotem ochrony prywatności i ograniczania nadzoru. Idea „interesu publicznego” jest również związana z tymi zagadnieniami pojęciowymi, zwłaszcza, w przypadku gdy prywatność i interes publiczny zajmują przeciwstawne pozycje w rozważaniach politycznych i prawnych, nie mówiąc już o debacie społecznej. Poważna analiza tych pojęć oraz ich relacji w poszczególnych kontekstach mogłoby pomóc we wsparciu sposobu, w jaki powołuje się na zasady prywatności i przekłada je na nowe sytuacje występujące w ramach „nowego nadzoru”. W przeciwnym razie prywatność i ograniczenie nadzoru będą prawdopodobnym przegranym w tym „konkursie”.
- Deбата społeczna: poziom debaty społecznej dotyczącej prywatności i nadzoru jest, ogólnie mówiąc, bardzo niski oraz, w niektórych krajach, z

pewnymi wyjątkami, lub w pewnych sytuacjach, jest on oderwany od aktualnych propozycji polityki rządowej lub innowacji handlowych. Wydaje się, że „Poważna” debata i debata społeczna to dwa odmienne światy, chociaż istnieje wiele blogów internetowych, w których toczy się ważna debata dotycząca aktualnych propozycji. Korzystne byłoby przeprowadzenie oceny obecnej roli konwencjonalnych i „nowych” mediów, organizacji obywatelskich i stowarzyszeń zawodowych, środowisk akademickich i innych podmiotów zaangażowanych w debatę, a także przekazywanie komunikatów zwiększających wiedzę społeczeństwa, jego świadomość i zachęcających do debaty wykraczającej poza często tendencyjne podejście dotyczące interesów gospodarczych i rządowych i grup nacisku mające na celu przeciąganie opinii publicznej z jednej strony na drugą. Taka ocena może przynieść usprawnienia; jednakże niebezpieczna podczas wdrażania tych usprawnień może okazać się tendencja do protekcyjnego traktowania i „oświecania” społeczeństwa, co w przypadku „publicznego rozumienia nauki” działa na niekorzyść sprawy.

- Obciążenia prawne: istnieją, oczywiście, koszty określania przepisów dotyczących prywatności i nadzoru oraz koszty utrzymania zgodności. Istnieje potrzeba przeprowadzenia niezależnej oceny tego, jakie są te koszty i kto je ponosi oraz dokonania osądu, na podstawie wyraźnych i ustalonych kryteriów, czy takie koszty są „nadmierne”, czy „przewyższają korzyści”, czy też rzeczywiście, jak często się im zarzuca, „ograniczają inicjatywę, podejmowanie ryzyka lub produktywność”. Z drugiej strony, korzyści wprowadzenia takich przepisów również wymagają przeprowadzenia surowej analizy. Można powiedzieć, że zdobycie społecznego zaufania i poprawa skuteczności organizacyjnej, jakie mogą wynikać w dobrej ochrony prywatności i uregulowania nadzoru zostały rozpoznane tylko w ograniczonym stopniu; jednakże one również wymagają przeprowadzenia bezstronnej analizy. Jednakże ekonomika (lub ekonomia polityczna, gdyż nie jest to problem czysto „ekonomiczny”, ale jedna z ogólnych wartości politycznych i społecznych) prywatności i nadzoru jest słabo rozwiniętą specjalnością i prawdopodobnie nie istnieje gotowy model, który mógłby zostać przyjęty bez znacznych dostosowań. Jeśli tak jest w rzeczywistości, stanowi to tak zwany trzeci etap: „równoważenie” kosztów i korzyści. Jesteśmy dalecy od twierdzenia, że dwuznaczna doktryna „równowagi”, która przenika praktykę i retorykę ochrony prywatności, może wytrzymać poważną kontrolę, ale powinna ona zostać jej poddana.³²³
- Dyskusja medialna: problem prywatności i nadzoru obecny w środkach przekazu wydaje się być zdominowany przez banały i nadmiernie uproszczony. Ostatnia „tragiczna sprawa” dotycząca tego, w jaki sposób błąd organizacji w analizie danych osobowych doprowadził do przypadków tragicznej śmierci lub (odwrotnie) jak „władze” tworzą ukradkiem ogromne bazy danych. Jak już wspomnieliśmy powyżej, należy wykorzystywać rolę, jaką odgrywają środki przekazu oraz rozważyć, jaką rolę będą mogły odgrywać w przyszłości. Złożone problemy społeczne i etyczne, a także osiągnięcia technologiczne, są trudne do omawiania na łamach prasy, w radiu czy telewizji i w innych mediach. Ponadto należy zauważyć, że podobnie jak w innych

³²³ Raab, C. (1999) „From balancing to steering: New directions for data protection [Od balansowania po kierowanie: Nowe kierunki w ochronie danych]”, w Bennett i Grant (ed.) (1999), *op cit.* nr 299.

przypadkach “społeczeństwo” jak i “środki przekazu” są podzielone i wysoce zróżnicowane. Takie problemy stanowią ogromny test dla wszelkich prób podniesienia poziomu, jaki reprezentują komunikaty środków przekazu.

- 45.3.3. Na koniec należałoby nawiązać do sposobu, w jaki przepisy prawne mogłyby zostać ulepszone poprzez rozważania nad stopniem dostosowania relacji i współzależności zadań pomiędzy systemami regulacyjnymi na różnych poziomach, w tym na poziomie światowym, a także pomiędzy różnymi rodzajami uczestnika w tym organami regulacyjnymi a grupami społeczeństwa obywatelskiego. Poprzez to pytanie, chcieliśmy nawiązać do telekomunikacji. Trudno jest rozważać ten problem w sposób abstrakcyjny, jednakże sprawą wymagającą odrębnego omówienia jest na przykład to, jak dalece współpraca, o której jest mowa w dyrektywie UE 95/46/WE posłużyła w celu nie tylko egzekwowania prawa i zapewnienia zgodności z prawem, ale również w celu gromadzenia informacji i zwiększania świadomości dotyczącej szerzej pojętego frontu praktyk i technologii nadzoru. Lub na przykład, jak dalece sięgają wzajemnie korzystne relacje zachodzące pomiędzy organami regulacyjnymi a grupami społeczeństwa obywatelskiego, jeżeli grupy te przekazują im sprawy i użyteczne informacje lub wiedzę i działają jak „osa”, w przypadkach gdy przepisy prawne wydają się słabnąć lub gdy praktyki rządowe i gospodarcze wydają się zwiększać nadzór. To, czy istnieje miejsce na dalsze innowacje w roli systemu prawodawczego, poza zaangażowanymi organami prawodawczymi i zagorzałymi przeciwnikami nadzoru, stanowi oddzielny problem, który należy zbadać poza niniejszym raportem, który być może okaże się pomocny w tych rozważaniach.