GRUPA ROBOCZA ART. 29

00727/12/PL
WP 192

Opinia 02/2012 w sprawie systemów rozpoznawania twarzy w usługach *online* i usługach komórkowych

Przyjęta w dniu 22 marca 2012 r.

Niniejsza grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określa art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Sekretariat grupy mieści się w Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, Dyrekcja C (Prawa podstawowe i obywatelstwo Unii Europejskiej), B-1049 Brussels, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_pl.htm

1. Wprowadzenie

W ostatnich latach nastąpił gwałtowny wzrost dostępności i precyzyjności technologii rozpoznawania twarzy. Ponadto technologia ta znalazła zastosowanie w dziedzinie usług *online* i usług komórkowych w celu identyfikacji i kategoryzacji osób oraz uwierzytelnienia/weryfikacji ich tożsamości. Technologia, która do niedawna stanowiła temat fantastyki naukowej, jest obecnie dostępna zarówno dla organizacji publicznych, jak i prywatnych. Jest ona wykorzystywana w dziedzinie usług *online* i usług komórkowych na przykład w portalach społecznościowych i przez producentów smartfonów.

Zdolność do automatycznego odczytu danych i rozpoznawania twarzy na podstawie obrazu cyfrowego poruszono wcześniej w dokumencie roboczym na temat biometrii Grupy Roboczej Art. 29 (GR29) i w niedawno opublikowanej opinii 03/2012 (GR193) w sprawie rozwoju technologii biometrycznych. Uważa się, że technologia rozpoznawania twarzy wchodzi w zakres biometrii, ponieważ w wielu przypadkach daje ona szczegóły wystarczające do precyzyjnej identyfikacji danej osoby.

W opinii 03/2012 stwierdza się, że:

> „[biometria] umożliwia zautomatyzowane obserwowanie, śledzenie lub tworzenie charakterystyki danych osób, a co za tym idzie, jej potencjalny wpływ na prywatność i prawo do ochrony danych osobowych jest wysoki".

To stwierdzenie odnosi się szczególnie do przypadku rozpoznawania twarzy w usługach *online* i usługach komórkowych, kiedy można zarejestrować obraz danej osoby (będącej świadomą lub nieświadomą tego faktu) i przesłać go na zdalny serwer w celu dalszego przetwarzania. Usługi *online*, których właścicielami i operatorami są często organizacje prywatne, zgromadziły ogromne zasoby danych w postaci obrazów, przesłane przez osoby, których te dane dotyczą. W niektórych przypadkach obrazy te uzyskano niezgodnie z prawem poprzez wykorzystywanie innych publicznych stron internetowych, takich jak pamięć podręczna wyszukiwarek internetowych. Małe urządzenia przenośne z aparatami fotograficznymi o wysokiej rozdzielczości umożliwiają rejestrowanie obrazów i przesyłanie ich w czasie rzeczywistym do usług *online* w trybie połączenia transmisji danych, które jest aktywne przez cały czas. W konsekwencji użytkownicy mogą udostępniać te obrazy innym, przeprowadzić identyfikację lub kategoryzację znanych lub nieznanych sobie osób widniejących na obrazie, lub też uwierzytelnić/zweryfikować ich tożsamość w celu uzyskania dodatkowych informacji o tych osobach.

Technologia rozpoznawania twarzy w usługach *online* i usługach komórkowych wymaga zatem szczególnej uwagi ze strony GR29, ponieważ jej zastosowanie niesie ze sobą szereg obaw związanych z ochroną danych.

Celem tej opinii jest rozważenie ram prawnych i zapewnienie odpowiednich zaleceń właściwych dla technologii rozpoznawania twarzy, kiedy ta stosowana jest w kontekście usług *online* i usług komórkowych. Opinia ta skierowana jest do europejskich i krajowych organów legislacyjnych, administratorów danych i użytkowników tego rodzaju technologii. Opinia nie ma na celu powtarzania zasad, o których mowa w opinii 03/2012, a raczej oparcie się na nich w zakresie usług *online* i usług komórkowych.

2. Definicje

Technologia rozpoznawania twarzy nie jest pojęciem nowym i istnieje wiele definicji i interpretacji związanej z nią terminologii. Z tego względu warto jasno zdefiniować technologię, której dotyczy niniejsza opinia.

Obraz cyfrowy: Obraz cyfrowy jest odzwierciedleniem dwuwymiarowego obrazu w formie cyfrowej. Najnowsze osiągnięcia z zakresu technologii rozpoznawania twarzy wymagają jednak dołączenia trójwymiarowych obrazów do obrazów statycznych, jak i tych zawierających obrazy ruchome (tzn. fotografie, nagrane materiały filmowe i materiały filmowe przesyłane na żywo).

Rozpoznawanie twarzy: Rozpoznawanie twarzy jest automatycznym przetwarzaniem obrazów cyfrowych zawierających twarze osób w celu ich identyfikacji, kategoryzacji lub uwierzytelniania/weryfikacji[1] ich tożsamości. Proces rozpoznawania twarzy składa się z kliku podprocesów:

a) Rejestrowanie obrazu: proces rejestrowania twarzy danej osoby i przekształcania jej w formę cyfrową (obraz cyfrowy). W przypadku usługi *online* lub usługi komórkowej obraz można zarejestrować w inny sposób, tzn. robiąc zdjęcie aparatem cyfrowym, które jest następnie przesyłane do usługi *online*.

b) Wykrywanie twarzy: proces wykrywania występowania twarzy na obrazie cyfrowym i zaznaczanie tego obszaru.

c) Ujednolicanie: proces niwelowania różnic w obrębie wykrytego obszaru przedstawiającego twarz, tzn. zmiana rozmiaru na standardowy, obrócenie obrazu lub skorygowanie rozmieszczenia kolorów.

d) Wydobycie cech charakterystycznych: proces wyodrębniania i przesyłania powtarzalnych i charakterystycznych cech z obrazu cyfrowego danej osoby. Wydobycie cech charakterystycznych może być całościowe,[2] oparte na konkretnych elementach[3] lub może być połączeniem tych dwóch metod[4]. Zespół głównych cech może być przechowywany jako wzór do zastosowania przy późniejszych porównaniach[5].

e) Wprowadzenie do systemu: jeżeli dana osoba po raz pierwszy została poddana procesowi rozpoznawania twarzy, obraz jej twarzy lub wzór mogą być przechowywane jako podstawa do późniejszych porównań.

---

1 Identyfikację, uwierzytelnienie/weryfikację i kategoryzację zdefiniowano w opinii 03/2012.

2 Wydobycie cech charakterystycznych oparte na metodzie całościowej: matematyczne odwzorowanie całego obrazu, takie jak w drodze analizy głównych składowych.

3 Wydobycie cech charakterystycznych oparte na konkretnych elementach: rozpoznanie umiejscowienia poszczególnych części twarzy, takich jak: oczy, nos czy usta.

4 Znane również jako metoda hybrydowa wydobycia cech charakterystycznych.

5 Wzór zdefiniowano w opinii 03/2012 jako „główne cechy wydobyte z nieprzetworzonej formy danych biometrycznych (tzn. wymiary dotyczące twarzy pobrane z obrazu) i przechowywane do celów późniejszego przetwarzania, raczej niż same nieprzetworzone dane".

f) Porównanie: proces badania podobieństwa między danym zespołem cech (próbką) a zespołem cech poprzednio wprowadzonym do systemu. Głównym celem porównania jest identyfikacja osób i uwierzytelnienie/weryfikacja ich tożsamości. Trzecim celem porównania jest kategoryzacja osób, będąca procesem wydobywania cech z obrazu przedstawiającego daną osobę, aby ją zaklasyfikować do jednej lub kilku szerszych kategorii (takich, jak: wiek, płeć, kolor stroju itd.). System kategoryzacji nie wymaga procesu wprowadzania osób do systemu.

3. Przykłady zastosowania technologii rozpoznawania twarzy w usługach *online* i usługach komórkowych

Technologia rozpoznawania twarzy może znaleźć wiele różnorakich zastosowań w dziedzinie usług *online* i usług komórkowych. W kontekście niniejszej opinii GR29 koncentruje się na kilku różnych przykładach mających zapewnić dodatkowe informacje na potrzeby analizy prawnej i dotyczących zastosowania technologii rozpoznawania twarzy w celach identyfikacji, uwierzytelniania/weryfikacji i kategoryzacji.

3.1. Rozpoznawanie twarzy jako sposób identyfikacji

Przykład 1: serwis społecznościowy[6] pozwala użytkownikom dołączyć obraz cyfrowy do ich profilu. Ponadto użytkownicy mogą przesyłać obrazy w celu udostępniania ich innym zarejestrowanym lub niezarejestrowanym użytkownikom. Zarejestrowani użytkownicy mogą samodzielnie identyfikować i oznaczać inne osoby (które mogą być zarejestrowane lub niezarejestrowane) na przesłanych obrazach. Takie oznaczenie może być widoczne dla osoby, która go dokonała, udostępnione szerszej grupie znajomych lub wszystkim zarejestrowanym lub niezarejestrowanym użytkownikom. Portale społecznościowe mogą używać oznaczonych obrazów w celu stworzenia wzoru dla każdego zarejestrowanego użytkownika i przy zastosowaniu systemu rozpoznawania twarzy, automatycznie sugerować oznaczenia w przypadku nowych obrazów przesyłanych przez tych użytkowników.

Dostęp do obrazów osób upublicznionych przez użytkowników można uzyskać przy użyciu wyszukiwarek internetowych, w których pamięci podręcznej są one przechowywane. Operatorzy wyszukiwarek mogą zdecydować się na udoskonalenie funkcji wyszukiwania poprzez zaoferowanie użytkownikom, po przesłaniu przez nich obrazu danej osoby, znalezienia zbliżonych wyników w formie obrazów, jak również wyszukania połączenia do profilu danej osoby na portalu społecznościowym. Obraz może być zarejestrowany aparatem fotograficznym w smartfonie i bezpośrednio z niego przesłany.

3.2. Rozpoznawanie twarzy jako sposób uwierzytelnienia/weryfikacji tożsamości

Przykład 2: system rozpoznawania twarzy jest stosowany w celu zastąpienia systemu dostępu do usług *online* lub usług/urządzeń komórkowych opartych na zalogowaniu przy użyciu nazwy użytkownika i hasła. Podczas rejestracji aparat fotograficzny wbudowany w urządzenie rejestruje obraz upoważnionego użytkownika tego urządzenia i powstaje w ten sposób wzór przechowywany na tym urządzeniu lub na zdalnie na serwerze. Aby uzyskać dostęp do usługi lub urządzenia, rejestruje się nowy obraz osoby próbującej uzyskać dostęp i porównuje się go do obrazu przechowywanego w systemie. Dostęp zostaje przyznany, jeżeli system potwierdzi zgodność obu obrazów.

[6] Pojęcie serwisu społecznościowego zdefiniowano ogólnie w opinii 05/2009 na temat portali społecznościowych jako „platformy komunikacyjne *on-line* umożliwiające osobom fizycznym przystępowanie do lub tworzenie sieci użytkowników o wspólnych upodobaniach".

3.3. Rozpoznawanie twarzy jako sposób kategoryzacji

Przyklad 3: portale społecznościowe opisane w przykładzie 1 mogą przyznać licencję na dostęp do zbioru obrazów stronie trzeciej, świadczącej usługi rozpoznawania twarzy *online*. Usługa ta pozwala klientom strony trzeciej na włączenie technologii rozpoznawania twarzy do swoich produktów. W rezultacie za pomocą tych produktów można przesyłać obrazy osób w celu wykrycia i skategoryzowania twarzy w oparciu o ustalone kryteria, takie jak wiek, płeć czy nastrój.

Przyklad 4: w konsolach do gier stosuje się systemy kontroli gestów, polegające na wykrywaniu ruchów użytkownika w celu zapewnienia mu kontroli nad grą. Aparaty fotograficzne wykorzystywane w systemach kontroli gestów przesyłają obrazy przedstawiające użytkowników gry do systemu rozpoznawania twarzy, który oszacowuje ich prawdopodobny wiek, nastrój oraz płeć. Uzyskane w ten sposób dane, jak i te pozyskane przy użyciu innych multimodalnych czynników, mogą zmodyfikować grę w celu podwyższenia komfortu obsługi użytkownika lub zmienić środowisko gry w celu dopasowania go do prawdopodobnego profilu użytkownika. W podobny sposób system może sklasyfikować użytkowników, aby przyznać/odebrać dostęp do części gry dopasowanych do odbiorców w określonym wieku lub aby wyświetlić wbudowane w gry reklamy dopasowane do konkretnych odbiorców.

4. Ramy prawne

Właściwe ramy prawne dla systemów rozpoznawania twarzy zawarte są w dyrektywie w sprawie ochrony danych (95/46/WE), które omówiono w opinii 03/2012. Niniejsza część ma na celu jedynie streszczenie ram prawnych w kontekście technologii rozpoznawania twarzy stosowanej w usługach *online* i usługach komórkowych w oparciu o przykłady podane w części 3. Dodatkowe przykłady dotyczące technologii rozpoznawania twarzy znajdują się w opinii 03/2012.

4.1. Obrazy cyfrowe jako dane osobowe

Kiedy obraz cyfrowy zawiera twarz danej osoby, która jest w pełni widoczna i umożliwia identyfikację tej osoby, obraz ten traktuje się jako dane osobowe. Taka klasyfikacja zależy od wielu czynników, takich jak jakość obrazu lub konkretny punkt obserwacji. Za dane osobowe w większości przypadków nie będą uznane obrazy przedstawiające osoby widziane z odległości lub których twarze są na obrazie nieostre. Warto jednak zauważyć, że obrazy cyfrowe mogą zawierać dane osobowe więcej niż jednej osoby (tak jak w przykładzie 4, gdzie w obrębie jednego obrazu mogło znajdować się kilku użytkowników gry) i obecność innych osób może świadczyć o istniejącym między nimi związku.

Opinia 04/2007 w sprawie pojęcia danych osobowych potwierdza, że jeżeli dane odnoszą się do „cech lub zachowania danej osoby lub też jeśli informacje te determinują lub też wpływają na sposób traktowania lub ocenę danej osoby", to są one traktowane jako dane osobowe.

Według definicji wzór tworzony na podstawie obrazu danej osoby również zalicza się do danych osobowych, ponieważ zawiera zbiór charakterystycznych cech twarzy danej osoby, który jest następnie kojarzony z konkretną osobą i przechowywany jako odniesienie dla dalszych porównań w celu identyfikacji i uwierzytelniania/weryfikacji tożsamości.

Wzór lub zbiór charakterystycznych cech używany jedynie w systemie kategoryzacji na ogół nie zawiera informacji wystarczających do zidentyfikowania danej osoby. Powinny one zawierać jedynie informacje konieczne do przeprowadzenia kategoryzacji (np. ze względu na płeć). W tym przypadku nie będą one uznane za dane osobowe, pod warunkiem że wzór (lub

wynik kategoryzacji) nie jest powiązany z wpisem, profilem lub pierwotnym obrazem danej osoby (które wciąż stanowią dane osobowe).

Ponadto, jako że wzory i obrazy cyfrowe przedstawiające osoby związane są z „cechami biologicznymi, aspektami behawioralnymi, cechami psychologicznymi, cechami życiowymi lub powtarzającymi się czynnościami, gdzie te cechy lub czynności są zarówno charakterystyczne wyłącznie dla tej osoby, jak i wymierne”[7], należy je uznać za dane biometryczne.

4.2. Obrazy cyfrowe jako szczególna kategoria danych osobowych

Obrazy cyfrowe przedstawiające ludzi mogą w niektórych przypadkach być uznane za szczególną kategorię danych osobowych[8]. Szczególnie gdy wzory lub obrazy cyfrowe przedstawiające ludzi są dodatkowo przetwarzane w celu otrzymania szczególnych kategorii danych, byłyby one z pewnością zaliczone do tej kategorii. Przykładem takiego zastosowania może być chęć otrzymania informacji na temat pochodzenia etnicznego, wyznania lub kondycji zdrowotnej danych osób.

4.3. Przetwarzanie danych osobowych w kontekście systemów rozpoznawania twarzy

Systemy rozpoznawania twarzy opierają się na określonej liczbie zautomatyzowanych etapów przetwarzania, jak opisano powyżej. Z tego powodu rozpoznawanie twarzy stanowi zautomatyzowaną formę przetwarzania danych osobowych, łącznie z danymi biometrycznymi.

W związku ze stosowaniem danych biometrycznych systemy rozpoznawania twarzy mogą podlegać dodatkowym kontrolom lub różnym przepisom prawnym w poszczególnych państwach członkowskich, takich jak wcześniejsze zezwolenie lub prawo pracy. Stosowanie biometrii w kontekście zatrudniania omówiono bardziej szczegółowo w opinii 03/2012.

4.4. Administrator danych

Na podstawie podanych przykładów administratorami danych są na ogół właściciele stron internetowych lub dostawcy usług internetowych, jak również operatorzy aplikacji na telefony komórkowe, którzy stosują systemy rozpoznawania twarzy przez określenie celów lub sposobów przetwarzania[9]. Jest to zgodne z wnioskiem zawartym w opinii 05/2009 w sprawie portali społecznościowych, w którym jest mowa o tym, że „dostawcy SNS [portali społecznościowych] są administratorami danych na mocy dyrektywy o ochronie danych”.

4.5. Uzasadnienie

Dyrektywa 95/46/WE ustanawia warunki, które muszą być spełnione w procesie przetwarzania danych osobowych. Oznacza to, że przetwarzanie musi być po pierwsze zgodne z wymogami dotyczącymi jakości danych (art. 6). W tym przypadku obrazy cyfrowe przedstawiające ludzi i ich wzory muszą być „stosowne” oraz „nienadmierne ilościowo” w stosunku do celów przetwarzania zmierzającego do rozpoznawania twarzy. Ponadto tego rodzaju przetwarzanie jest możliwe jedynie pod warunkiem spełnienia jednego z kryteriów określonego w art. 7.

---

7 Definicja danych biometrycznych oparta na opinii 03/2012.

8 W orzecznictwie niektórych krajów klasyfikuje się obrazy cyfrowe jako szczególną kategorię danych – LJN BK6331 Sąd Najwyższy Holandii z dnia 23 marca 2010 r.

9 Zobacz Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”.

Z względu na szczególne rodzaje zagrożeń związanych z danymi biometrycznymi, powyższe działania będą wymagały uzyskania świadomej zgody danej osoby przed rozpoczęciem przetwarzania obrazów cyfrowych w celu rozpoznania twarzy. W niektórych przypadkach administrator danych może jednak przejściowo być zmuszonym do wykonania części działań związanych z przetwarzaniem zmierzającym do rozpoznania twarzy, aby ocenić, czy użytkownik nie wyraził zgody czy też ją wyraził, co stanowi podstawę prawną przetwarzania. To wstępne przetwarzanie (tzn. rejestrowanie obrazu, wykrywanie twarzy, porównanie itd.) może w tym przypadku mieć osobną podstawę prawną, w szczególności uzasadniony interes administratora danych do stosowania się do zasad ochrony danych. Dane przetworzone w toku tych etapów mogą być użyte wyłącznie w ściśle ograniczonym celu, tj. weryfikacji zgody użytkownika, i dlatego powinny być wykasowane bezpośrednio po jej dokonaniu.

W przykładzie 1 administrator danych ustalił, że wszystkie nowe obrazy przesłane przez zarejestrowanych użytkowników portali społecznościowych zostaną poddane procesom wykrywania twarzy, wyodrębnienia cech i porównania. Jedynie zarejestrowani użytkownicy posiadający wzór obrazu wprowadzony do identyfikacyjnej bazy danych zostaną skojarzeni z nowymi obrazami i w ten sposób otrzymają automatycznie wskazywane oznaczenie. Jeżeli zgoda danej osoby byłaby uznana za jedyną możliwą podstawę prawną przetwarzania obrazów, cała usługa musiałaby zostać wstrzymana, ponieważ nie ma możliwości uzyskania, na przykład, takiej zgody od niezarejestrowanych użytkowników, których dane osobowe mogłyby być przetwarzane podczas etapów wyrywania twarzy i wyodrębniania cech charakterystycznych. Ponadto nie byłoby możliwe rozróżnienie zarejestrowanych użytkowników, którzy wyrazili zgodę i tych, którzy jej nie wyrazili bez uprzedniego przeprowadzenia rozpoznania twarzy. Jedynie po dokonaniu identyfikacji tych osób (lub w wypadku niepowodzenia identyfikacji) administrator danych mógłby stwierdzić, czy posiada on wymaganą zgodę na dany proces przetwarzania.

Zanim zarejestrowany użytkownik prześle obraz do portalu społecznościowego, musi być jasno poinformowany, że te obrazy będą wykorzystywane w systemie rozpoznawania twarzy. Co więcej, należy zagwarantować zarejestrowanym użytkownikom dodatkowy wariant polegający na wyrażeniu zgody lub jej braku na wprowadzenie wzoru ich obrazu do identyfikacyjnej bazy danych. Imiona i nazwiska niezarejestrowanych i zarejestrowanych użytkowników, którzy nie wyrazili zgody na przetwarzanie obrazów, nie będą zatem automatycznie wskazywane do oznaczenia, ponieważ wyszukiwanie obrazów, które będą ich przedstawiały, da wynik typu „brak rezultatu”.

Nie należy mylić zgody udzielonej przez osobę przesyłającą zdjęcie z potrzebą istnienia podstawy prawnej do przetwarzania danych osobowych innych osób widniejących na danym obrazie. W tym celu administrator danych może zastosować inną podstawę prawną do przetwarzania na etapach pośrednich (wykrywanie twarzy, ujednolicanie i porównanie), która byłaby w uzasadnionym interesie administratora danych, pod warunkiem że zastosowane będą odpowiednie ograniczenia i kontrole w celu ochrony podstawowych praw i wolności podmiotów danych niebędących osobami, które przesłały obrazy. Takie mechanizmy kontrolne obejmowałyby zagwarantowanie, że z momentem uzyskania wyniku wyszukiwania typu „brak rezultatu”, nie będą zachowywane żadne dane powstałe w toku przetwarzania (tzn. wszystkie wzory i związane z nimi dane zostaną w sposób pewny zniszczone). Administrator danych może również rozważyć zapewnienie użytkownikom narzędzia pozwalającego na zamazanie twarzy osób, które nie zostaną dopasowane do wzoru w referencyjnej bazie danych w toku przesyłania obrazów. Wprowadzenie wzoru obrazu danej osoby do identyfikacyjnej bazy danych (umożliwiając tym samym skojarzenie obrazów i sugestie co do oznaczenia) byłoby możliwe jedynie po uzyskaniu świadomej zgody podmiotu danych.

W przykładzie 2 pokazana jest wyraźna możliwość uzyskania zgody osoby posiadającej dostęp do urządzenia podczas procesu wprowadzania danych. Aby zgoda była ważna, należy stworzyć alternatywny, równie bezpieczny system kontroli dostępu (np. oparty na trudnym do złamania haśle). Ten alternatywny, sprzyjający ochronie prywatności wariant powinien być wariantem domyślnym. Kiedy dany użytkownik przedstawia się przed kamerą podłączoną do urządzenia w wyraźnym celu uzyskania dostępu, można uznać, że osoba ta wyraziła zgodę na przetwarzanie danych związanych z obrazem jej twarzy w celu weryfikacji tożsamości, nawet jeśli ta osoba nie jest upoważnionym użytkownikiem tego urządzenia. Poziom uzyskanych informacji musi być jednak wystarczający, żeby zagwarantować, że zgoda jest ważna.

Dodatkowe ulepszenia zbioru zdjęć portali społecznościowych opisane w przykładzie 3 byłyby wyraźnym przypadkiem złamania ograniczenia celu i dlatego dana osoba musi wyrazić ważną zgodę przed wprowadzeniem takiej usługi, wyraźnie zaznaczając, że takie przetwarzanie obrazów będzie miało miejsce. To samo odnosi się do wyszukiwarek internetowych opisanych w przykładzie 1. Obrazy otrzymane w wyniku wyszukiwania pokazywane były w celu oglądania, a nie na potrzeby systemu rozpoznawania twarzy. Operator wyszukiwarki musiałby otrzymać zgodę od podmiotów danych na wprowadzenie ich danych do drugiego systemu rozpoznawania twarzy.

To samo odnosi się do przykładu 4, ponieważ użytkownik może nie spodziewać się, że obrazy zarejestrowane w celu kontroli gestów będą podlegały dalszemu przetwarzaniu. Jeżeli administrator danych wnosi o zgodę na przetwarzanie danych w dłuższej perspektywie (np. przez dłuższy okres lub w różnych grach), musi on dopilnować, by użytkownicy otrzymywali regularne przypomnienia na temat działania systemu i domyślnej możliwości jego wyłączenia.

W opinii 15/2011 w sprawie definicji zgody omówiono kwestie jakości, dostępności i widoczności informacji związanych z przetwarzaniem danych osobowych. W opinii stwierdza się, że:

> „informacje trzeba przedstawić bezpośrednio osobom fizycznym. Nie wystarcza, aby były one *gdzieś dostępne*".

Z tego powodu informacje związane z funkcją rozpoznawania twarzy w usługach *online* lub usługach komórkowych nie powinny być ukryte, ale udostępnione w przystępny i zrozumiały sposób. Należy również zagwarantować, że kamery nie będą działały w ukryty sposób. Stosując technologię rozpoznawania twarzy, administratorzy danych powinni uwzględnić zrozumiałe oczekiwania użytkowników dotyczące ochrony prywatności, i w odpowiedni sposób zaradzić ich obawom.

W tym kontekście zgoda na wprowadzenie do bazy danych nie może być efektem zaakceptowania przez użytkownika ogólnych warunków związanych z podstawowymi usługami, chyba że główny cel tej usługi związany jest z rozpoznawaniem twarzy. Dzieje się tak dlatego, że w większości przypadków wprowadzenie do bazy będzie dodatkową funkcją, niezwiązaną bezpośrednio z działaniem danej usługi *online* lub usługi komórkowej. Użytkownicy mogą nie spodziewać się, że taka funkcja jest aktywowana podczas korzystania z danej usługi. W tym celu należy w jasny sposób zagwarantować użytkownikom możliwość wyrażenia zgody na tę funkcję albo podczas rejestracji albo na późniejszym etapie, zależnie od tego, kiedy funkcja pojawia się w usłudze.

Aby zgoda mogła być uznana za ważną, należy podać stosowne informacje na temat przetwarzania danych. Należy zapewnić użytkownikom możliwość wycofania zgody w prosty sposób przez cały czas korzystania z usługi. W momencie wycofania zgody należy natychmiast zaprzestać przetwarzania danych mającego celu rozpoznanie twarzy.

5. Szczegółowe uwagi i zalecenia

Zagrożenia dla prywatności ze strony sytemu rozpoznawania twarzy są uwarunkowane całkowicie rodzajem stosowanego przetwarzania i jego celu/-ów. Istnieją jednak pewne zagrożenia właściwe konkretnych etapom procesu rozpoznawania twarzy. Niniejsza część podkreśla główne zagrożenia i przedstawia stosowne zalecenia dotyczące najlepszych praktyk.

5.1. Niezgodne z prawem przetwarzanie w celu rozpoznania twarzy

W środowisku *online* administrator danych może wchodzić w posiadanie obrazów na wiele różnych sposobów, np. mogą być one przesyłane przez użytkowników usługi *online* lub usługi komórkowej, przez ich znajomych, współpracowników lub osoby trzecie. Obrazy te mogą przedstawiać twarze samych użytkowników lub innych zarejestrowanych albo niezarejestrowanych użytkowników. Mogą też być zarejestrowane bez wiedzy podmiotu danych. Niezależnie od sposobu, w jaki te obrazy znalazły się w posiadaniu administratora, wymagana jest podstawa prawna do ich przetwarzania.

Zalecenie 1: Jeżeli administrator danych rejestruje obrazy samodzielnie (np. tak jak w przykładach 2 i 4), musi zagwarantować, że posiada ważną zgodę podmiotu danych przed rejestracją obrazu i że udzieli wystarczających informacji związanych z tym, kiedy aparat fotograficzny jest włączony w celu rozpoznania twarzy.

Zalecenie 2: Jeżeli osoby rejestrują obrazy cyfrowe i przesyłają je do usług *online* i usług komórkowych w celu rozpoznania twarzy, administratorzy danych muszą zagwarantować, że osoby te zgodziły się na przetwarzanie tych obrazów, które może nastąpić w celu rozpoznania twarzy.

Zalecenie 3: Jeżeli administratorzy danych otrzymują obrazy cyfrowe osób fizycznych od osób trzecich (np. skopiowane ze strony internetowej lub nabyte od innego administratora danych), muszą oni uważnie zbadać ich źródło i okoliczności, w jakich nabyto i przetworzono obrazy, jedynie pod warunkiem, że podmioty danych wyraziły zgodę na przetwarzanie.

Zalecenie 4: Administratorzy danych muszą zagwarantować, że obrazy cyfrowe i wzory są używane wyłącznie w tym celu, w jakim zostały dostarczone. Administratorzy danych powinni wprowadzić kontrole techniczne, aby zmniejszyć ryzyko dalszego przetwarzania obrazów cyfrowych przez osoby trzecie w celach, na które użytkownik nie wyraził zgody. Administratorzy danych powinni zapewnić użytkownikom narzędzia do kontroli widoczności przesłanych przez nich obrazów, w których ustawieniem domyślnym jest ograniczenie dostępu dla osób trzecich.

Zalecenie 5: Administratorzy danych muszą zagwarantować, że obrazy cyfrowe osób fizycznych, które nie są zarejestrowanymi użytkownikami danej usługi lub nie wyrazili zgody na ich przetwarzanie, będą przetwarzane jedynie w takim zakresie, w jakim administrator ma uzasadniony interes do przetwarzania. Tak jak pokazano w przykładzie 1, administrator musi zaprzestać przetwarzania i wykasować wszystkie dane, jeżeli wyszukiwanie nie przyniesie pozytywnego rezultatu.

Naruszenie bezpieczeństwa podczas transmisji
W przypadku usług *online* i usług komórkowych istnieje prawdopodobieństwo, że nastąpi transmisja danych między etapem rejestracji obrazu i pozostałymi etapami przetwarzania (np. przesyłanie obrazu z aparatu fotograficznego na stronę internetową w celu wyodrębnienia cech charakterystycznych i porównania).

Zalecenie 6: Administrator danych musi podjąć odpowiednie kroki aby zapewnić bezpieczeństwo transmisji danych. Może to oznaczać zaszyfrowane kanały komunikacyjne lub zaszyfrowanie samego obrazu. W miarę możliwości i szczególnie w przypadku uwierzytelniania/weryfikacji tożsamości, należy przetwarzać dane na lokalnym serwerze.

5.2. Wykrywanie twarzy, ujednolicanie, wyodrębnianie cech charakterystycznych

Minimalizacja danych:
Wzory tworzone przez system rozpoznawania twarzy mogą zawierać więcej danych niż potrzeba do wykonania określonego celu lub określonych celów.

Zalecenie 7: Administratorzy danych muszą zagwarantować, że dane uzyskiwane z obrazu cyfrowego nie będą nadmierne ilościowo i będą zawierały jedynie te informacje niezbędne do wykonania określonego celu, unikając tym samym ewentualnego dalszego przetwarzania. Wzory nie powinny być przesyłane między różnymi systemami rozpoznawania twarzy.

Naruszenie bezpieczeństwa podczas przechowywania danych
Identyfikacja i uwierzytelnianie/weryfikacja wymagają na ogół przechowywania wzoru do późniejszych porównań.

Zalecenie 8: Administrator danych musi wybrać najbardziej odpowiednią lokalizację przechowywania danych. Może to być urządzenie użytkownika lub umiejscowienie w systemach administratora danych. Zalecenie 6: Administrator danych musi podjąć odpowiednie działania aby zapewnić bezpieczeństwo przechowywania danych. Może to oznaczać zaszyfrowanie wzoru. Nie powinno być możliwości uzyskania nieuprawnionego dostępu do wzoru lub lokalizacji jego przechowywania. Zwłaszcza w przypadku rozpoznawania twarzy w celu weryfikacji można zastosować techniki szyfrowania biometrycznego. W tych technikach klucz kryptograficzny jest bezpośrednio związany z danymi biometrycznymi i jest tworzony ponownie jedynie, jeśli w momencie weryfikacji zostanie przedstawiona poprawna próba danych biometrycznych. Nie ma potrzeby przechowywania obrazu ani wzoru (tworząc tym samym swego rodzaju „niewykrywalną biometrię").

Dostęp podmiotu

Zalecenie 9: Administrator danych powinien zapewnić podmiotom danych odpowiednie mechanizmy egzekwowania ich prawa dostępu do, w miarę potrzeb, pierwotnych obrazów oraz wzorów tworzonych w procesie rozpoznawania twarzy.

Sporządzono w Brukseli dnia 22 marca 2012 r.

W imieniu grupy roboczej
Przewodniczący
Jacob KOHNSTAMM