

Kontrola w stosunkach pracownik – pracodawca w RFN

Krótki rys

Jan Muszyński

Universität Bayreuth

Lehrstuhl für Öffentliches Recht IV

Universitätsstraße 30

D - 95447 Bayreuth

janmuszynski2003@gmail.com

Spis treści

Wstęp.....	1
Podstawy prawne.....	1
Ochrona danych osobowych pracownika.....	2
Regulacja § 32 BDSG	3
Kandydat na prześwietleniu	3
Dyscyplina musi być... ale uczciwość przede wszystkim	4
Kiedy wolno inwigilować?.....	4
Warunek 1	4
Warunek 2	5
Warunek 3 oraz 4	5
Sposoby kontroli, czyli co wolno pracodawcy.....	6
GPS, GPS-owi nie równy	6
Kontrola komputera.....	6
Monitoring w miejscu pracy	7
Podsumowanie	7

Wstęp

Podstawy prawne

Niemcy, jako państwo federalne posiadają dwa reżimy ochrony danych osobowych – **federalny oraz 16 systemów** w krajach związkowych, przy czym Federalna ustawa o ochronie danych osobowych (**Bundesdatenschutzgesetz**¹) obejmuje swym zakresem stosowania zarówno podmioty prywatnoprawne zajmujące się pozyskiwaniem, przetwarzaniem i wykorzystywaniem danych osobowych, jak i instytucje federalne. Ustawy poszczególnych krajów związkowych z kolei mają ograniczony zasięg terytorialny i znajdują zastosowanie tylko do podmiotów działających wyłącznie na terenie danego „Landu” (np. organów gmin, urzędów krajowych itd.). Z punktu widzenia niniejszego opracowania podział ten ma znaczenie, ponieważ pracodawcą mogą być zarówno instytucje państwowe jak i

¹ dalej: BDSG

podmioty prywatne, tak o zasięgu rozciągającym się na teren całej federacji, jak i o zasięgu lokalnym. Należy mieć tego świadomość zagłębiając się w wielopoziomowy, nie odpowiadający znanym z Polski prawidłom system prawny. Do tego należy wspomnieć o specjalnych regulacjach dotyczących danych osobowych pracowników służby cywilnej zarówno federalnych, jak i krajowych.

Kolejnym ważnym kompleksem regulacji w materii kontroli w stosunkach pracy, który należy wspomnieć jest indywidualne prawo pracy. W przeciwieństwie do Polski w Niemczech podstawowe przepisy prawa pracy nie zostały skodyfikowane w ramach jednego aktu prawnego - Kodeksu Pracy². Dlatego przepisów prawa pracy należy doszukiwać się w wielu ustawach, tak na poziomie federalnym, jak i krajowym. Jeśli chodzi o regulacje dotyczące uprawnień pracodawcy w materii pracowniczych danych osobowych należy wymienić ponad to **ustawę o telemediach (Telemediengesetz)**, **ustawę o federalne służbie cywilnej (Bundesbeamtengesetz)**, a także **ustawa o ustroju rad zakładowych (Betriebsverfassungsgesetz)**.

Ochrona danych osobowych pracownika

Temat ochrony danych osobowych pracownika czy też zgodnie z niemiecką terminologią „danych dotyczących osoby” (Personenbezogene Daten) definiowanych jako informacje dotyczące osobistych i faktycznych stosunków danej osoby identyfikujące ją bezpośrednio lub pozwalające na jej identyfikację (§ 4 ust. 1 BDSG) stał się bardzo popularny w latach 2007 - 2009 r. kiedy to wyszły na jaw trzy afery dotyczące szpiegowania pracowników w kilku niemieckich koncernach.

Sprawy te odbiły się szerokim echem w debacie społecznej, ponieważ pod prężaniem stanęły przedsiębiorstwa nie tylko zatrudniające i oferujące swoje usługi milionom obywateli, ale także cieszące się ich uznaniem. W ogniu krytyki pojawiły się Niemieckie Koleje (**Deutsche Bahn AG – DB AG**), **Deutsches Telekom** oraz **Lidl**. Wszystkie one prowadziły, jak to określała prasa, „akcje szpiegowskie” wymierzone nie tylko we własnych pracowników także najwyższych szczebli, a także w ich rodziny.

Na początku 2009 r. wyszło na jaw, że DB AG szpiegowała wręcz swoich pracowników, głównie by sprawdzić lojalność kadry menedżerskiej wobec pracodawcy. Wg tygodnika „Stern”³ ponad 1000 pracowników kolei miało być na przestrzeni wielu lat szpiegowanych na zlecenie DB AG przez firmę Netzwerk GmbH. Prześwietlane miały być kontakty pracowników, a także ich rodzin, by wykluczyć możliwość działań na szkodę firmy oraz korupcję. Działania prowadzone były przewencyjnie, bez żadnych udokumentowanych podejrzeń. Po ujawnieniu afery odpowiedzialne za nią osoby w DB AG bagatelizowały sprawę mówiąc, że nie zdawały sobie sprawy z nielegalności procedury.⁴

Rok 2009 i ostatnia afera Deutsche Bahn AG przelały czarę goryczy. W społeczeństwie, w którym już w latach osiemdziesiątych ubiegłego wieku rozgorzała dyskusja na temat ochrony danych osobowych w kontekście spisu powszechnego, temat prywatności i transparentności we wszelkich obszarach wiążących się z danymi osobowymi jest bardzo

² Mimo, że „Einigungsvertrag” – Traktat o zjednoczeniu NRF i NRD z 31 sierpnia 1990 r. to przewidywał.

³ <http://www.stern.de/wirtschaft/news/unternehmen/daten-skandal-bahn-bespitzelte-eigene-mitarbeiter-652179.html>

⁴ <http://www.youtube.com/watch?v=dseddLSUKew>

żywy⁵. Świadomość społeczeństwa co do doniosłości i wagi ujawnionych afer była duża, toteż oburzenie wśród Niemców na ogół bardzo ostrożnie i świadomie podchodzących do sprawy swoich danych osobowych⁶, było szczególne. Opinię publiczną tym bardziej bulwersował fakt, że w obliczu tak poważnych nadużyć oraz braku ustawodawstwa skutecznie chroniącego pracowników w tym zakresie rząd postanowił zająć się tematem dopiero po przypadających na wrzesień 2009r. wyborach do Bundestagu. Presja opinii publicznej spowodowała jednak, że mimo początkowego braku woli politycznej w parlamencie do wprowadzenia nowelizacji DBSG rząd RFN zdecydował się jednak przeprowadzić w ekspresowym tempie **nowelizację centralnego przepisu dotyczącego ochrony danych pracowników (Angestelltendatenschutz) - § 32 BDSG**. Nowelizacja weszła w życie 1 września 2009 r.

Regulacja § 32 BDSG

§ 32 BDSG jest centralnym przepisem dotyczącym ochrony danych osobowych osób wykonujących pracę – w dowolnej formie prawnej (umowa o pracę, zlecenie itd.) a także kandydatów do pracy.

W myśl tego przepisu „dane osobowe pracownika, mogą być pozyskiwane, przetwarzane lub wykorzystywane do celów zatrudnienia, jeżeli jest to konieczne do podjęcia decyzji o zatrudnieniu lub do wykonywania pracy lub do zakończenia stosunku pracy.”⁷ (§ 32 BDSG zd. 1). Jak więc wygląda to w praktyce?

Kandydat na prześwietleniu

Jednym z filarów niemieckiego prawa ochrony danych osobowych jest zasada bezpośredniego pozyskiwania informacji (§ 4 ust. 2 zd. 1 BDSG). Można jednak od niej odstąpić gdy „dane te są ogólnie dostępne [...] chyba, że godny ochrony interes zainteresowanego przewyższa w sposób nie pozostawiający wątpliwości interes czerpiącego informację.”⁸ (§ 28 ust. 1 nr. 3 BDSG). W przypadku „**Datamining**” uprawianego przez pracodawcę w powszechnie dostępnych zasobach Internetu sprawa nie jest prosta. Z jednej strony § 32 BDSG nie zakazuje wprost prowadzenia takich poszukiwań, z drugiej jednak przeprowadzenie wyważenia interesów kandydata i pracodawcy jest wyjątkowo trudne.⁹ Pozostaje to strefą starć między obrońcami prawa do prywatności, a obrońcami prawa do korzystania z informacji powszechnie dostępnych.

O ile zasoby powszechnie dostępne pozostają niejednoznacznie uregulowane, o tyle zasoby, do których uzyskuje się dostęp przez zalogowanie się na konkretnym portalu są chronione przed wścibskością pracodawcy. **Wyjątek** stanowią jednak media społecznościowe o wyraźnym nacechowaniu zawodowym i profesjonalnym (np. LinkedIn).

⁵ „Volksszählungsurteil” Federalnego Trybunału Konstytucyjnego (http://de.wikipedia.org/wiki/Volkssz%C3%A4hlung_in_Deutschland#Die_Volkssz.C3.A4hlung_von_1987)

⁶ Google streetview.

⁷ Tłumaczenie: J.M.

⁸ Tłumaczenie: J.M.

⁹ M. Franzen w: „Erfurter Kommentar zum Arbeitsrecht“; Kommentarz do art. 32 BDSG; 14. Auflage, Monachium 2014

Dyscyplina musi być... ale uczciwość przede wszystkim

W celu wykrywania czynów karalnych (w niemieckiej terminologii w tym przypadku dotyczy to nie tylko przestępstw, ale również, a nawet przede wszystkim zwykłych dyscyplinarnych uchybień w pracy) dane dotyczące osoby zatrudnionej mogą być pozyskiwane, przetwarzane i wykorzystywane, gdy istnieje **realne, uzasadnione i udokumentowane podejrzenie** popełnienia czynu karalnego w ramach stosunku zatrudnienia. Pozyskiwanie, przetwarzanie i wykorzystywanie tych danych może być przedsięwzięte wyłącznie, jeśli jest to **konieczne** do wykrycia czynu karalnego oraz gdy **godny ochrony interes osoby zatrudnionej** nie przeważa nad interesem (pracodawcy) w ujawnieniu czynu karalnego, w szczególności gdy ciężar gatunkowy czynu karalnego w sposób oczywisty jest **nieproporcjonalny** do powziętych środków do jego wykrycia (§ 32 ust. 1 BDSG).

Przepis ten skonstruowany jest w bardzo interesujący sposób. Dopuszcza kontrolowanie pracownika w jego miejscu pracy, przykładowo kontrolę komputera służbowego, monitoring miejsca pracy, czy inne tym podobne sposoby kontroli jednak tylko w ściśle określonych przypadkach. Przepis jest jednocześnie na tyle elastyczny i pojemny, że komentatorzy i orzecznictwo zauważają trudność w abstrakcyjnym ujęciu stanu faktycznego podpadającego pod ten przepis. Każdorazowa subsumcja musi być poprzedzona szczegółową analizą danego przypadku ponieważ znamiona określające zastosowanie § 32 BDSG są bardzo ocenne. Praktyka dostarcza jednak dużej ilości przykładów, a rozpowszechnianie ich przebiega bardzo sprawnie poprzez portale z orzecnictwem sądów, prasę fachową oraz często wznawiane i aktualizowane komentarze.

Kiedy wolno inwigilować?

Warunek 1

Warunkiem wstępnym prowadzenie szeroko zakrojonej kontroli pracownika w jego miejscu pracy przy użyciu środków technicznych jest przede wszystkim **realne i udokumentowane podejrzenie popełnienia czynu karalnego**. Oznacza to, że pracodawca musi najpierw powziąć podejrzenie o sprzecznych z obowiązkami pracowniczymi zachowaniami pracownika.

W tym celu dopuszczalne jest prowadzenie wrywkowych kontroli w miejscu pracy – także za pomocą urządzeń technicznych (nagrywanie dźwięku, obrazu, sprawdzanie zawartości komputera) warunkiem legalności takich **wrywkowych kontroli** (Stichprobe) jest zgoda pracownika.

Specyficzny dla tego typu kontroli jest zakaz prowadzenia ich w sposób ciągły, a jedynie dokonywanie ich wrywkowo i to tylko w przypadkach, w których pracownik wyraził na to zgodę uprzednio zgodę. W praktyce stosuje się formularze zgody, a faktycznie raczej karty informujące o kontrolach, wymieniające komputer służbowy, telefon, pomieszczenie w którym wykonywana jest praca. Pracodawca jest umocowany do tego, by stwierdzać naruszenie dyscypliny, nie może jednak zapisywać treści tego typu poczynań pracownika jeśli dotyczą one jego prywatnych spraw. Programy śledzące aktywność na danym komputerze, rejestrujące operacje i teksty wprowadzane za pomocą klawiatury, ukryte mikrofony te wszystkie urządzenia w miejscu pracy znajdują usprawiedliwienie wyłącznie gdy informowany jest o tym pracownik (w niektórych przypadkach także rada zakładowa) oraz

gdy spełnione są pozostałe warunki z § 32 BDSG – o których poniżej. Granica między zgodną z prawem inwigilacją a nielegalnym szpiegostwem jest wyjątkowo cienka. Jej przestrzeganie leży jednak w interesie pracodawcy, gdyż gdy dojdzie do nałożenia kary dyscyplinarnej pracownik będzie miał prawo zweryfikowania legalności kontroli, która doprowadziła do wykrycia jego wykroczeń dyscyplinarnych także przez sąd pracy. Korzystanie z „owoców zatrutego drzewa” będzie dla niego nie tylko kontraproduktywne, ale może w skrajnych przypadkach spowodować skierowanie przeciwko niemu postępowania karnego.

Warunek 2

Gdy dojdzie już do wykrycia przewinienia dyscyplinarnego pracownika koniecznym jest stwierdzenie jego **ciężaru gatunkowego**. Jeżeli przewinienie nie jest na tyle poważne, by kontynuować kontrolę i w dalszym ciągu zbierać informacji dotyczące jego popełnienia pracodawca powinien zaniechać kontroli. Tylko w przypadku, w którym interes pracodawcy w ukaraniu i ukróceniu procedury łamania dyscypliny w zakładzie pracy przeważa nad interesem pracownika w ochronie jego danych osobowych uzasadnionym jest kontynuowanie kontroli w celu zdobycia dowodów do ukarania pracownika. Wiąże się z tym absolutny zakaz gromadzenia i wykorzystywania prywatnych treści generowanych, nawet w sposób naruszający dyscyplinę, przy użyciu służbowego komputera. Pracodawca ma prawo zarejestrować fakt naruszenia dyscypliny zakładowej np. poprzez wejście na stronę portalu społecznościowego i zalogowanie się na prywatne konto, nie może natomiast infiltrować treści jakie zamieszcza pracownik podczas danej sesji chociażby w prywatnych wiadomościach, ani zapisywać i gromadzić loginów oraz haseł do wykorzystywanych przez pracownika portali.

Warunek 3 oraz 4

W Niemczech wielką rolę przypisuje się zasadzie proporcjonalności, tak w prawie konstytucyjnym czy administracyjnym – skąd się wywodzi, jak i coraz częściej w prywatnym. Orzecznictwo dotyczące **wyważania interesów** i formuł tych wyważań jest w tym kraju wyjątkowo bogate. Także w przypadku interesu pracodawcy w zachowaniu dyscypliny w zakładzie pracy, a interesem pracownika w utrzymaniu prywatności należy posłużyć się swoistym testem proporcjonalności. Przepis § 32 BDSG przewiduje jednak tylko w ograniczonym zakresie (nie tak obszernie jak ma to miejsce w prawie administracyjnym) zastosowanie tej metody. Otóż zbieranie danych musi być **konieczne** w celu wykrycia uchybień dyscyplinarnych. Oznacza to, że korzystanie z ”technik szpiegowskich” wobec pracownika może mieć miejsce tylko gdy w inny sposób nie będzie możliwe wykrycie jego przewinień dyscyplinarnych i potwierdzenie przypuszczeń pracodawcy. Ponadto stosowanie tego typu metod musi być **proporcjonalne** – czyli interes pracodawcy, ingerującego w prawo podstawowe pracownika, a dobrem chronionym – prywatnością pracownika, nie pozostają w dysproporcji.

Przepis § 32 BDSG jest przepisem, jak już wspominałem, bardzo specyficznym ze względu na swoją niedookreśloność. Należy jednak zauważyć, że orzecznictwo i jurysprudencja niemiecka przyczynia się w sposób twórczy do rozwoju jego interpretacji. Jest to niezmiernie ważne, ponieważ w ten sposób wyznaczane są spójne granice interpretacji prawa. W tym przypadku to szczególnie istotne, gdyż nieostre granice zastosowania § 32 BDSG mogłyby dawać pole do nadużyć interpretacyjnych.

Co ciekawe, trzeba oddać niemieckiemu ustawodawcy, że w przeciwieństwie do polskiego nie odwołuje się do jeszcze bardziej ocennych i nacechowanych ładunkiem emocjonalnym pojęć np. godności ludzkiej (11¹ KP), co w niewątpliwie pozytywny sposób wpływa na praktykę stosowania § 32 BDSG. Doprecyzowane i zobiektywizowane przez doktrynę i orzecznictwo podczas wieloletniej praktyki pojęcia konieczności (Erforderlichkeit), proporcjonalności (Verhältnismäßigkeit) czy też interesu chronionego (schutzwürdiges Interesse) sprzyjają interpretowaniu wspomnianego przepisu w sposób generalny, abstrakcyjny i spójny oczywiście przy uwzględnieniu indywidualnych cech każdego stanu faktycznego.

Sposoby kontroli, czyli co wolno pracodawcy

W poprzednich punktach postarałem się przedstawić pokrótce w jakiej sytuacji pracodawca może kontrolować swego pracownika. Gdy już to wiadomo należy zastanowić się przy pomocy jakich środków może on to robić?

GPS, GPS-owi nie równy

Z jednej strony pracodawca ma prawo i obowiązek wymagać, by jego pracownik efektywnie wykorzystywał czas pracy. Z drugiej zaś jego naturalna skłonność do sprawdzenia wykorzystywania bądź, co bądź swoich środków nie może zagrażać w zbyt drastyczny sposób prywatności pracownika.

Pracodawca ma obowiązek poinformować pracownika o prowadzonych przez siebie kontrolach. Nie może to się jednak odbywać przez podsuniecie pracownikowi do podpisu formuły: „Wyrażam zgodę na kontrolowanie mnie w miejscu pracy.” O rozmiarach (co jest kontrolowane), czasie (jak często, bez podania dokładnej godziny lecz częstotliwości) i sposobach (pozostające do dyspozycji pracodawcy środki techniczne) pracownik zobowiązany jest zostać poinformowany.

Kontrola komputera

Służbowa skrzynka mailowa jest własnością pracodawcy, niemniej jednak pracownik musi wyrazić zgodę na przejęcie do niej dostępu przez pracodawcę. Prywatna skrzynka mailowa jest natomiast własnością pracownika. Co dzieje się jednak gdy sprawdza on i wysyła prywatne maile w godzinach pracy? Pracodawca ma prawo do korzystania z programów rejestrujących działania na komputerze służbowym, nie wolno mu jednak zapisywać prywatnych danych pracownika, nawet gdy wprowadza je do służbowego komputera wbrew w zasadom dyscypliny. PIN-y, loginy, hasła, treści maili pracowników muszą zostać usunięte z rejestru pracodawcy, nie jednak sam fakt ich wprowadzania. Podobnie ma się rzecz z korzystaniem ze służbowego telefonu.

Z samochodem służbowym sprawa ma się nieco odmiennie. Ostatnimi czasy pracodawcy bardzo narzekali za pośrednictwem mediów, że z samochodów służbowych najwięcej profitów ma pracownik mogący korzystać z niego prywatnie, a nie sam

pracodawca.¹⁰ Dlatego też w samochodach służbowych zaczęły pojawiać się odbiorniki GPS. Geolokacja pozwala pracodawcy w praktycznie non-stop sprawdzać położenie i prędkość należącego do niego pojazdu. Jednak taka ciągła kontrola nie jest legalna, gdyż zbyt głęboko inwigiluje prywatne życie pracownika – głównie po godzinach pracy. Oczywiście kontrolowanie stanu licznika czy wrywkowe sprawdzanie odbiornika GPS w godzinach pracy jest możliwe i legalne. Po jej godzinach natomiast niedopuszczalne. I tutaj obowiązuje jednak zasada informowania pracownika o kontrolach. Sprawa z montowaniem instrumentów do geolokacji w samochodach służbowych jest bardzo kontrowersyjna i trudna do interpretowania. Tym bardziej, że póki co nie pojawiło się jeszcze wyjaśniające orzeczenie najwyższej instancji sądów pracy w Niemczech - Bundesarbeitsgericht.

Monitoring w miejscu pracy

Podobnie jak w pozostałych przypadkach Niemiecki ustawodawca dopuszcza także monitoring w miejscu pracy. Rozróżnić należy jednak monitoring miejsc ogólnie dostępnych – także dla osób z zewnątrz zakładu, znajdujący się na korytarzach czy przy wejściu do siedziby firmy, od monitoringu miejsca pracy i miejsc o ograniczonym dostępie¹¹.

§ 6b BDSG reguluje umieszczenie monitoringu miejsc publicznych, w tym także w miejscach pracy uzależniając go od trzech czynników: po pierwsze gdy jest to konieczne do prawidłowego wykonywania zadań danego podmiotu, po drugie gdy ma to pomóc w przestrzeganiu regulaminu wewnętrznego instytucji, po trzecie gdy dzięki monitoringowi będą lepiej chronione cele i interesy danego podmiotu administrowanego monitoringiem. Czynniki te nie muszą występować zbiorczo. Wystarczy, że uprawdopodobni się jeden z powodów wymienionych w przepisie. Monitoring musi być odpowiednio oznakowany także przez oznaczenie podmiotu odpowiedzialnego za jego administrowanie. Dane w ten sposób pozyskane mogą być wykorzystywane tylko jeśli nie sprzeciwia się temu godny ochrony interes osób zainteresowanych.

Odmienne przedstawia się natomiast sprawa monitorowania miejsc nie dostępnych powszechnie w miejscu pracy – biur, pomieszczeń socjalnych itd. (Monitorowanie szatni i toalet jest zabronione). W tych przypadkach należy stosować się do wspomnianych regulacji § 32 BDSG.

Podsumowanie

Temat ochrony danych osobowych jako takich jest u naszego zachodniego sąsiada szeroko dyskutowany co najmniej od roku 1983, czyli od wyroku Federalnego Trybunału Konstytucyjnego dot. spisu powszechnego (Volkszählungsurteil). Od tamtego czasu temat ten przewija się przez różne dziedziny prawa od prawa administracyjnego, aż po prawo pracy. Zaowocowało to licznymi nowelizacjami i bogatą literaturą dotyczącą tej tematyki. Po nowelizacji ustawy o ochronie danych osobowych (BDSG) w 2009 r. także w dziedzinie prawa pracy wzmocniono ochronę prywatności pracownika.

Godnym pochwały zabiegiem niemieckiego ustawodawcy jest stworzenie regulacji, która jest jednocześnie elastyczna i obiektywna – dzięki zastosowaniu pojęć nieostrych

¹⁰ Profity z samochodu służbowego artykuł

¹¹<http://www.bfdi.bund.de/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Video%20BCberwachung.html?nn=409756>

pozwała na dopasowaną subsumcję do danego stanu faktycznego, a jednocześnie przez znaczący dorobek orzecznictwa i doktryny prawa daje pewność i ścisłe ramy interpretacyjne. Nie pojawiają się w tekście ustawy odwołania do nacechowanych emocjonalnie pojęć „godności ludzkiej” czy „wolności”, albo też „prywatności”, ponieważ ustawodawca uznał, że ich nieokreślona, płynna i w różnych systemach wartości odmiennie interpretowana treść będzie stanowić problem w procesie codziennego stosowania prawa.