

MONITORING W SIECIACH HANDLOWYCH

ZŁODZIEJ TEŻ MA PRAWO DO OCHRONY WIZERUNKU?

Sieci handlowe wymieniają się zapisami z monitoringu, aby skuteczniej ścigać złodziei – doniosły niedawno niektóre media. Czy faktycznie tak jest i czy takie praktyki są legalne? Okazuje się, że sieć może się powołać na szczególne okoliczności.

Do Generalnego Inspektora Ochrony Danych Osobowych (GIODO) nie docierały do tej pory sygnały dotyczące takich praktyk. Nie znając zatem szczegółów i biorąc pod uwagę to, że w polskim porządku prawnym brak jest całościowego unormowania kwestii stosowania monitoringu wizyjnego (istnieją jedynie regulacje szcztątkowe, odnoszące się np. do wykorzystywania go w działalności policji czy straży gminnych), można się do tego odnieść jedynie teoretycznie. Tym bardziej że brak jest również przepisów uwzględniających specyfikę tego rodzaju przetwarzania danych w ustawie o ochronie danych osobowych. Zatem stosowanie jej przepisów jest możliwe w ograniczonym zakresie i może dotyczyć tylko niektórych sytuacji związanych z monitoringiem. Wymiana danych osobowych, czyli ich udostępnienie, jest jedną z form przetwarzania, a więc w zależności od tego, kto jest administratorem danych – czy sklep, czy sieć handlowa – to po stronie tego podmiotu istnieje obowiązek podania podstawy prawnej takiego działania. Przyjmując więc, że w czasie monitoringu wizyjnego dochodzi do przetwarzania danych osobowych, to każdy, kto jest ich administratorem, musi legitymować się jedną z przesłanek dopuszczalności przetwarzania danych z art. 23 ust. 1 ustawy.

Należy do nich m.in. zgoda osoby, której dane dotyczą, przepis prawa lub prawnie usprawiedliwiony cel administratora danych, jeżeli przetwarzanie takich danych nie narusza praw i wolności osoby, której dane dotyczą. W pewnych przypadkach odpowiednią podstawą udostępnienia danych osobowych innemu podmiotowi może być również zawarta na piśmie pomiędzy tym podmiotem a administratorem danych umowa powierzenia przetwarzania danych, o której mowa w art. 31 ustawy. Jak wskazuje art. 31 ust. 2 tej ustawy, podmiot taki może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Zatem podmiot, któremu powierzono przetwarzanie danych, jest związany w swej działalności zakresem i celem przetwarzania w przedmiotowej umowie wyznaczonym. Istotą powierzenia jest fakt, że nie działa się w swoim imieniu, lecz w imieniu i na rzecz administratora danych. Dodatkowo podmiot ten jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, czyli m.in. zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć

dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, a także nadać upoważnienia osobom dopuszczonym do przetwarzania danych osobowych. Jednocześnie wskazać należy, że stosowanie unormowań ustawy o ochronie danych osobowych należy w pierwszej kolejności do administratorów danych, których wspierać w tym mogą m.in. administratorzy bezpieczeństwa informacji (ABI), o ile zostaną w danym podmiocie powołani. To administrator danych jest bowiem obowiązany respektować wszelkie nałożone na niego przepisami prawa obowiązki związane z procesem przetwarzania danych osobowych. Potwierdza to art. 36b ustawy o ochronie danych osobowych, który stanowi, że w razie niepowołania administratora bezpieczeństwa informacji administrator danych sam wykonuje zadania określone w art. 36a ust. 2 pkt 1, a więc także musi zapewnić, że przepisy o ochronie danych osobowych są przestrzegane. Za ich naruszenie przewidziana jest odpowiedzialność karna, stosownie do przepisów rozdziału 8 ustawy. I tak przykładowo, kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 49). Natomiast, kto administrując zbiorem danych lub będąc obowiązany do ochrony danych osobowych udostępnia je lub umożliwia dostęp do nich osobom nieupoważnionym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2 (art. 51). Każdy podmiot, który uważa, że jego prawa zostały naruszone, może także złożyć skargę do GIODO. Intencje, jakie przyświecają poszkodowanym handlowcom można zrozumieć, należy się jednak liczyć z określonymi w prawie konsekwencjami takich działań. W rezultacie to oni bowiem mogą zostać pociągnięci do odpowiedzialności za naruszenie dóbr osobistych domniemanego złodzieja. Wynika to z faktu, że wizerunek człowieka – jako jedno z dóbr osobistych – pozostaje pod ochroną prawa cywilnego, niezależnie od ochrony przewidzianej



Podobne zdjęcia na witrynach sklepów nie są odosobnionym przypadkiem

w innych przepisach. W rezultacie taka osoba może próbować dochodzić roszczeń z tytułu naruszenia dóbr osobistych na drodze sądowej, w trybie przewidzianym przepisami ustawy z dnia 17 listopada 1964 roku Kodeks postępowania cywilnego. Przy czym przepisy o ochronie dóbr osobistych osób fizycznych stosuje się odpowiednio do osób prawnych (art. 43 Kodeksu cywilnego). Jednocześnie należy wskazać na wyrok Sądu Najwyższego z dnia 3 grudnia 2010 roku (sygn. akt I CSK 95/10), który uznał, że ujęta w art. 24 Kodeksu cywilnego ochrona dóbr osobistych przysługuje jedynie przed bezprawnym zagrożeniem lub naruszeniem dobra osobistego, a stwierdzenie, czy miały miejsce okoliczności wyłaczające bezprawność zachowania naruszającego dobro osobiste, dokonywane być powinno przy uwzględnieniu wszystkich okoliczności konkretnego przypadku. Sąd uznał, że „nie każde naruszenie dobra osobistego stanowi podstawę udzielenia ochrony prawnej podmiotowi dotkniętemu naruszeniem, ponieważ warunkiem jej przyznania jest uznanie, że naruszenie to miało bezprawny charakter”. Podmiot usprawiedliwiający swoje działanie – w tym wypadku sieć handlowa – może zatem powoływać się na szczególne okoliczności uprawniające do jego podejmowania.



Małgorzata Kałużyńska-Jasak, dyrektor zespołu rzecznika prasowego GIODO

NIE WIERZĘ W KOOPERACJĘ SIECI HANDLOWYCH

Współpracując z sieciami i handlowymi i trudno mi uwierzyć, że wymieniają się one zapisami z monitoringu. I dyrektorzy sklepów, i ochroniarze mają świadomość, jakie konsekwencje grożą za naruszenie wizerunku klienta, nawet jeśli jest on złodziejem. Stanowisko Generalnego Inspektora Ochrony Danych Osobowych jest jasne – do zapisów z monitoringu może mieć dostęp tylko policja czy prokuratura i tego się w branży trzymamy. Jeśli już miałoby dojść do jakiegoś wymieniania się zdjęciami złodziei, to między sklepami tej samej sieci, ale na pewno nie jest tak, że sieć A dogaduje się z siecią B i osoby mające dostęp do zapisów z monitoringu przekazują sobie nawzajem materiały. Byłoby to zbyt ryzykowne, a sieci sobie nie ufają, trudno ufać konkurencji. Są inne, legalne sposoby ograniczania kradzieży, np. rotacja pracowników – sprzyja to eliminowaniu złodziei, którzy chodzą kraść od sklepu do sklepu.

Tomasz Grabski, prezes Polskiego Stowarzyszenia Pracowników Ochrony