CZASOPISMO PRAWA KARNEGO
I NAUK PENALNYCH
Rok XIII: 2009, z. 2 ISSN 1506-1817

GERARD KARP

ANALIZA PRAWNOKARNEJ ODPOWIEDZIALNOŚCI ADMINISTRATORA DANYCH JAKO GWARANTA NIENASTĄPIENIA SKUTKU ZA PRZESTĘPSTWA MATERIALNE POPEŁNIONE PRZEZ ZANIECHANIE

Administrator danych, a więc podmiot (organ, instytucja, jednostka organizacyjna lub osoba), który decyduje o celach i środkach przetwarzania danych osobowych może samodzielnie dokonywać ich przetwarzania lub, w określonym zakresie, powierzyć takie działania innemu podmiotowi, tzw. procesorowi. Takie zlecenie przetwarzania danych „na zewnątrz" znajduje podstawę normatywną w art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[1] (dalej: o.d.os.), który przewiduje szczególne obowiązki po stronie administratora danych zamierzającego powierzyć procesorowi przetwarzanie danych, jak również określa zobowiązania leżące po stronie procesora.

W świetle wzrastającej roli usług outsourcingowych, gdzie pewne czynności zlecane są do podmiotów zewnętrznych ustalenie zasad wzajemnej współpracy pomiędzy zlecającym przetwarzanie danych administratorem danych a podmiotem przetwarzającym te dane na zlecenie, tj. procesorem oraz w szczególności ustalenie odpowiedzialności za powierzone dane jest niebagatelna, gdyż może wpływać bezpośrednio na zakres odpowiedzialności, w tym prawnokarnej zarówno procesora, jak również samego administratora danych. Przykładowo powszechną aktualnie praktyką stosowaną przez podmioty gospodarcze jest powierzanie przetwarzania danych pracowników na potrzeby np. zarządzania wypłatami wynagrodzeń

[1] Dz.U. z 2002 r., Nr 926, poz. 101 ze zm.

tzw. payroll podmiotom świadczącym tego typu usługi. Podobnie podmioty, które korzystają z serwerów tzw. hosting providerów powierzają im przechowywanie własnych treści, w tym częstokroć danych osobowych. Wszędzie zatem tam, gdzie dochodzi do przekazywania danych osobowych w celach realizacji określonych usług w imieniu podmiotów przekazujących dane — administratorów powinny być przez tych ostatnich podjęte pewne określone czynności mające zagwarantować szeroko pojęte bezpieczeństwo przetwarzanych danych. W powyższych przypadkach administratorzy danych powinni m.in. zawrzeć z podmiotami, które wykonują w ich imieniu określone czynności, tj. usługi payrolu lub hostowania treści, co najmniej stosowne umowy powierzenia przetwarzania danych. Brak takich umów zawartych między administratorem a procesorem jest złamaniem prawnie określonych obowiązków i powinno być postrzegane jako niedochowanie należytej staranności przez administratora danych. Z kolei stwierdzenie zaniedbania obowiązków — nie tylko przez brak zawarcia umowy powierzenia przetwarzania danych, po stronie administratora danych — może prowadzić, pod pewnymi warunkami, do rozważenia jego prawnokarnej odpowiedzialności w przypadku dokonanych naruszeń postanowień ustawy o ochronie danych osobowych przez procesora, w szczególności w sytuacji wywołania przez tego ostatniego przestępnego skutku.

Rozważania na temat prawnokarnej odpowiedzialności administratora danych miałyby dotyczyć dopuszczenia przez tegoż — wskutek zaniechania podjęcia określonych działań, do których był obowiązany — do wystąpienia skutku spowodowanego nie przez niego samego, lecz przez procesora, któremu powierzył on przetwarzanie danych osobowych.

Dla przyjęcia jakiejkolwiek odpowiedzialności prawnokarnej koniecznym jest — zgodnie z zasadą *nullum crimen sine lege poenali* — istnienie wyraźnej podstawy prawnej odpowiedzialności, którą dla przestępstw materialnych popełnionych przez zaniechanie stanowi na gruncie obowiązującego Kodeksu karnego art. 2. W jego świetle odpowiedzialności karnej za przestępstwo skutkowe popełnione przez zaniechanie może podlegać ten tylko, na kim ciążył prawny, szczególny obowiązek zapobiegnięcia skutkowi[2].

Artykuł 2 k.k. reguluje odpowiedzialność jedynie za przestępstwa skutkowe (materialne) popełnione przez zaniechanie. W zakres działania po-

---

[2] A. Zoll, w: G. Bogdan, Z. Ćwiąkalski, P. Kardas, J. Majewski, J. Raglewski, M. Szewczyk, W. Wróbel, A. Zoll, *Kodeks karny. Część ogólna*, t. 1: *Komentarz do art. 1–116*, red. A. Zoll, Kraków 2004, tezy 1 i 2 do art. 2.

wyższego artykułu nie wchodzą przestępstwa charakteryzujące się brakiem wystąpienia skutku tzw. przestępstwa formalne. Na płaszczyźnie podmiotowej konstrukcja art. 2 k.k. daje możliwość przypisania przestępnego skutku zarówno w przypadku przestępstw umyślnych, jak również nieumyślnych popełnionych przez gwaranta. Strona podmiotowa jest jednym z elementów odróżniających odpowiedzialność na gruncie art. 2 k.k. od pomocnictwa do popełnienia określonego czynu zabronionego stanowiącego odrębny typ czynu zabronionego (art. 18 § 3 k.k.).

Problematyka odpowiedzialności gwaranta za skutek spowodowany działaniem lub zaniechaniem podmiotu trzeciego należy do prawnokarnego zagadnienia odpowiedzialności za pracę (skutek przestępny) powstały w wyniku pracy w zespole. Choć analizowana sytuacja, zakładająca odpowiedzialność administratora danych za skutek spowodowany działaniem/zaniechaniem procesora, nie mieści się w klasycznie ujęte ramy problematyki odpowiedzialności za pracę w zespole i w związku tym zastosowanie prostej kalki przyjętych konstrukcji jest trudne do zaakceptowania, to jednak nie ulega wątpliwości, iż określone podobieństwa istnieją i w związku z tym pewne rozwiązania *per analogiam* mogą zostać zaakceptowane. Klasyczny problem odpowiedzialności za pracę w zespole dotyczy tych sytuacji, gdzie zaniechanie wywiązania się z obowiązków jednego z uczestników procesu pracy wpływa na poziom wykonania obowiązków przez tych uczestników, którzy wykonują swe zadania w obrębie tego zaniechania[3]. Nie ulega wątpliwości, iż kluczowym zagadnieniem w przypadku odpowiedzialności gwaranta za skutek spowodowany przez osobę trzecią w ramach pracy zespołowej jest ustalenie każdorazowo treści obowiązków gwaranta. Podział pracy, a więc również obowiązków, wiąże się ściśle z konsekwencjami w dziedzinie odpowiedzialności[4]. Zorganizowanie pracy

---

[3] G. R e j m a n, w: *Kodeks karny. Część ogólna. Komentarz*, red. G. Rejman, Warszawa 1999, teza 8 do art. 2.

[4] *Ibid*., teza 8 do art. 2. Autor na gruncie orzeczenia SN z 24 IX 1952 r., IV/K/107, OSN 1953, nr 1, poz. 7 analizuje odpowiedzialność kierownika laboratorium farmaceutycznego za błąd laborantki. W powyższym orzeczeniu SN przyjął, iż zwierzchnik pracy jest zobowiązany do właściwej organizacji pracy, do ustalenia w taki sposób ram pracy, ażeby błąd na szczeblu wykonawczym był niemożliwy. Zorganizowanie w sposób nie wykluczający pomyłki takiej pracy obciąża tego, kto wadliwie przygotował stanowisko pracy, a nie tego kto dopuścił się pomyłki. Choć SN nie posłużył się sformułowaniem naruszenia określonych reguł ostrożności przez zwierzchnika, to wydaje się, że właśnie taka konstatacja jest jak najbardziej uprawniona. Mianowicie, zwierzchnik powinien był dopełnić określonych obowiązków w postaci właściwej organizacji pracy. Niedopełniając faktycznie tychże obowiązków naruszył stosowne reguły ostrożności ad-

musi przebiegać w ten sposób, ażeby wykluczona była możliwość pomyłki przez personel pomocniczy. Źle zorganizowany zakład pracy stwarza niebezpieczeństwo wadliwego wykonania zadań przez osoby w nim zatrudnione, a przez to stwarza niebezpieczeństwo, które przy powstaniu dodatkowych okoliczności może się przekształcić w skutek zabroniony przez ustawę karną[5]. Słusznie w literaturze zwraca się uwagę, iż ustalenie obowiązku organizacji pracy spoczywającego na określonym podmiocie nie daje jasnej odpowiedzi, iż w każdym przypadku wystąpienia przestępnego skutku gwarant będzie ponosił odpowiedzialność karną za skutek[6]. Trudno jest, bowiem w takich sytuacjach ocenić, czy doszło, do konkretyzacji obowiązku gwaranta. Innymi słowy trudno jest odpowiedzieć na pytanie, czy każde zaniedbanie obowiązków przez personel pomocniczy gwaranta może skutkować jego odpowiedzialnością, czy tylko takie uchybienia, które związane są z jego obowiązkami, których nie mógł nikomu powierzyć. Odpowiedź na powyższe pytanie musi być poprzedzona właściwą analizą struktury organizacyjnej danego podmiotu, w ramach którego doszło do wystąpienia skutku przestępnego będącego konsekwencją bezpośrednich działań/zaniechań personelu pomocniczego. Nie ulega wątpliwości, iż uznanie, że w ramach określonej struktury, określony podmiot (chodzi o jeszcze inny podmiot niż sam gwarant) jest odpowiedzialny za zabezpieczenie konkretnego dobra przez chociażby właściwą organizację pracy, będzie prowadziła do zwolnienia z odpowiedzialności samego gwaranta na rzecz właśnie tego podmiotu[7]. Próba oceny odpowiedzialności gwaranta będzie się wiązała

---

resowane właśnie do niego i tym samym naruszył normę statuującą obowiązek gwaranta nienastąpienia skutku. Jeżeli dalej byśmy powiedzieli, że właśnie naruszenie tychże reguł ostrożności pozostawało w związku normatywnym ze skutkiem oraz wystąpienie takiego skutku było przewidywalne, droga do przypisania skutku zwierzchnikowi pozostaje otwarta.

5 Orzeczenie SN z 27 X 1983 r., II KR 219/83, OSPIKA 1984, nr 11, na gruncie którego SN analizował odpowiedzialność karną lekarza (ordynatora) za skutek (śmiertelny) spowodowany przez pielęgniarkę poprzez zaaplikowanie pacjentom niewłaściwych środków medycznych.

6 G. R e j m a n, w: *Kodeks*..., *op. cit*., teza 9 do art. 2.

7 *Ibid*., teza 10 do art. 2, autor analizując na gruncie orzeczenia SN z 27 X 1983 r., II KR 219/83, OSPIKA 1984, nr 11 odpowiedzialność ordynatora za skutek spowodowany przez pielęgniarkę, stwierdza iż „[…] należy wziąć pod uwagę strukturę organizacyjną oddziału ginekologicznego szpitala. Przyjmują zatem hipotetycznie, że na oddziale ginekologicznym, którym kierował pociągnięty do odpowiedzialności karnej ordynator, były wydzielone służby farmakologiczne, należałoby stwierdzić, że odpowiadać powinien nie on, lecz pracownik dbający o właściwe przechowywanie środka dezynfekującego. Innymi słowy chodzi o to czy ordynator, który wypisać zlecenie wydania

również z oceną, jakiej czynności dotyczył błąd. Jeżeli skutek był wynikiem błędu mieszczącego się w ramach kompetencji podmiotu go wywołującego, odpowiedzialność gwaranta wydaje się być trudna do obrony. Z kolei, sytuacja gdzie błąd był związany z czynnościami przekraczającymi kompetencje tego personelu, albo gdy personel pomocniczy nie posiadał odpowiednich kwalifikacji wtedy odpowiedzialność gwaranta mogłaby być rozważana[8]. Odpowiedzialność każdego z uczestników pracy zespołowej bada się z punktu naruszenia obiektywnych reguł ostrożności odnoszących się do poszczególnych członków zespołu, a reguły te mogą być różne dla poszczególnych członków pracy zespołowej[9]. Stosowanie powyższych zasad ustalenia odpowiedzialności podmiotu (gwaranta) za skutek wywołany przez podmiot trzeci (różnego typu personel pomocniczy) może być niezmiernie pomocne przy próbie odpowiedzi na pytanie o zakres odpowiedzialności administratora danych za skutek spowodowany przez procesora. Nie ulega wątpliwości, iż konstrukcja normatywna przepisów ustawy o ochronie danych osobowych daje podstawy do przyjęcia, iż administrator danych jest pewnego rodzaju zwierzchnikiem działań podejmowanych w jego imieniu i na jego rzecz przez procesora, który pełni rolę swoistego rodzaju podmiotu wspomagającego proces przetwarzania danych. Można pokusić się o stwierdzenie, iż procesor pełni rolę podmiotu pomocniczego w realizacji działań zamierzonych przed administratora. W związku z powyższym, lecz tylko na zasadzie pewnej analogii do odpowiedzialności za pracę w zespole, zasady te mogą być pomocne w analizie odpowiedzialności administratora za skutek spowodowany przez procesora.

---

azotynu sodu do celów dezynfekcyjnych, miał jeszcze obowiązek zadbania o to, aby ten środek był właściwie przechowywany przez służbę aptieczną. Uznanie, że ordynator jest odpowiedzialny za wadliwe przechowywanie przez niego środków dezynfekujących, nie byłoby tak oczywiste gdyby funkcjonował specjalny punkt farmakologiczny, do którego obowiązków należałyby właśnie tego typu sprawy. Poszczególne struktury organizacyjne powołuje się przecież w celu odciążenia pracowników włączonych w proces leczenia (np. ordynatora wypisującego zlecenie) od czynności pomocniczych, takich jak każdorazowe sprawdzanie, czy pielęgniarka wzięła zaordynowany specyfik. Wydzielenie wyspecjalizowanych służb, których istota polega na dbaniu o właściwe przechowywanie środków medycznych i dezynfekujących, konsumuje obowiązek ordynatora sprawdzania wszystkich czynności personelu mu podporządkowanego. W innym, bowiem, wypadku organizacja pracy i jej podział nie miałyby żadnego merytorycznego znaczenia ponieważ błędami personelu wyspecjalizowanego automatycznie obciążano by kierownika".

[8] G. R e j m a n, w: *Kodeks...*, *op. cit.*, teza 10 do art. 2.

[9] A. Z o l l, *Odpowiedzialność karna lekarza za niepowodzenie w leczeniu*, Warszawa 1988, s. 86.

Warunkiem koniecznym podjęcia prób rozważenia potencjalnej odpowiedzialności karnej administratora danych na gruncie art. 2 k.k. za skutek spowodowany przez procesora jest ustalenie, w pierwszej kolejności, że ustawa o ochronie danych osobowych przewiduje jakikolwiek typ czynu zabronionego znamienny skutkiem. Odpowiedź negatywna prowadziłaby automatycznie do wykluczenia możliwości przyjęcia odpowiedzialności karnej administratora danych za skutek spowodowany przez procesora. W przypadku braku przestępstwa o charakterze skutkowym odpowiedzialność karna administratora danych mogłaby być przedmiotem oceny na gruncie przepisu art. 18 § 3 k.k. określającego odpowiedzialność karną gwaranta nienastąpienia skutku za realizację znamion pomocnictwa przez zaniechanie. W takim przypadku warunkiem pociągnięcia administratora danych (gwaranta) do odpowiedzialności karnej byłaby realizacja przez niego znamion pomocnictwa[10] określonych właśnie artykułem 18 § 3 k.k.[11]

Artykuł 51 ust. 1 o.d.os. przewiduje, iż „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 lub pozbawienia wolności do lat 2". Zgodnie z art. 51 ust. 2 o.d.os., odpowiedzialność karna grozi również sprawcy w przypadku nieumyślnej realizacji przez niego znamion tego konkretnego przestępstwa.

Realizacja znamion typu czynu zabronionego opisanego w art. 51 ust. 1 o.d.os. musi nastąpić w jednej z dwóch form: przez udostępnienie danych osobowych lub umożliwienie dostępu do nich osobom nieupoważnionym. Właśnie pierwsza z wymienionych form, tj. „udostępnianie danych", konstytuuje typ przestępstwa materialnego[12]. Udostępnianie może być zreali-

---

[10] Musiałoby dojść do realizacji znamion zarówno podmiotowych pomocnictwa, czyli po stronie sprawcy musiałby wystąpić zamiar realizacji znamion pomocnictwa, jak i znamion przedmiotowych — w tym przynajmniej jednej z form czasownikowych przewidzianych w art. 18 § 3 k.k.

[11] Zob. szerzej P. K a r d a s, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, tezy 157, 164 do art. 18 § 3 k.k.

[12] Za przyjęciem materialnego charakteru znamienia czasownikowego „udostępniać" opowiadają się J. B a r t a, P. F a j g i e l s k i, R. M a r k i e w i c z, *Ochrona danych osobowych. Komentarz*, Kraków 2004, s. 739; H. D w u l a t, *Odpowiedzialność karna administratora danych z art. 51 ustawy o ochronie danych osobowych*, „Radca Prawny" 2003, z. 5, s. 55. Za odmiennym podejściem i przyjęciem formalnego charakteru przestępstwa opowiada się A. A d a m s k i, *Prawo karne komputerowe*, Warszawa 2000, s. 164; R. Z a k r z e w s k i, M. O r g a n i ś c i a k, *Ochrona danych osobowych — przepisy karne*, „Przegląd Ustawodawstwa Gospodarczego" 2002, z. 8, s. 19; B. K u r z ę p a,

zowane w różnych formach. Należy zauważyć, iż pojęciem „udostępniać" posługuje się również ustawa o dostępie do informacji publicznej[13].

Skutek — rozumiany jako taka zmiana w świecie zewnętrznym, którą da się oddzielić od samego zachowania się sprawcy[14] — w postaci udostępnienia można rozumieć jako taki stan rzeczywistości, w którym dane zostały obiektywnie udostępnione i nastąpiło zapoznanie się z danymi osobowymi przez co najmniej jednego „nieupoważnionego odbiorcę"[15]. Autor niniejszego opracowania stoi na stanowisku, iż skutek w postaci udostępnienia zachodzi również wtedy, gdy nie doszło do zapoznania się z danym przez podmiot nieupoważniony, ale udostępnienie przybrało taką formę, że zapoznanie się z treścią danych nie napotyka najmniejszych przeszkód. Faktycznie, skutkiem w postaci udostępnienia byłoby już samo wręczenie nośnika zawierającego dane osobowe, gdyby dostęp do nich nie wymagał dodatkowych czynności np. odkodowania zabezpieczonego pliku. Natomiast znamię czasownikowe „umożliwia dostęp", należy rozumieć jako stworzenie potencjalnej możliwości zapoznania się z danymi np. niezabezpieczenie sprzętu informatycznego przed nieupoważnionym dostępem do danych. Innymi słowy, np. wręczenie nośnika z danymi jest ich udostępnieniem i stanowi samo w sobie skutek przestępny, natomiast brak stosownych zabezpieczeń jest jedynie stworzeniem pewnych możliwości dostępu do danych osobowych. Obie formy „udostępniać" i „umożliwiać dostęp" różnią się też formą realizacji czynu zabronionego[16]. Przyjęcie, iż typ czynu zabronionego określony w art. 51 ust. 1 o.d.os. konstytuuje typ materialny przestępstwa, prowadzi — zgodnie z tym, co powiedziano już wcześniej — do możliwości pociągnięcia — przy spełnieniu warunków przypisywalności skutku w przypadku zaniechania — na gruncie art. 2 k.k. administratora danych jako gwaranta nienastąpienia skutku do odpowiedzialności karnej za skutek spowodowany przez podmiot trzeci, tj. procesora.

Przestępstwa z ustawy o ochronie danych osobowych, PiP 1999, z. 6, s. 51; por. również postanowienie SN z 11 XII 2000 r., II KKN 438/2000, OSNKW 2001, nr 3/4, poz. 33.

[13] Ustawa z dn. 6 IX 2001 r. o dostępie do informacji publicznej, Dz.U. 2001, Nr 112, poz. 1198 ze zm. Zgodnie z art. 7 w zw. art. 10 i 11 tejże ustawy udostępnienie informacji publicznej może nastąpić w drodze:
a) ogłoszenia informacji publicznej np. w Biuletynie Informacji Publicznej,
b) udostępnienia w formie pisemnej lub ustnej,
c) w drodze wyłożenia lub wywieszenia,
d) przez zainstalowanie urządzenia umożliwiającego zapoznanie się z tą informacją.

[14] K. B u c h a ł a, A. Z o l l, *Polskie prawo karne*, Warszawa 1995, s. 152 i n.

[15] J. B a r t a, P. F a j g i e l s k i, R. M a r k i e w i c z, *op. cit.*, s. 739.

[16] Zob. A. A d a m s k i, *op. cit.*, s. 164.

Odpowiedzialność za przestępstwa materialne popełnione przez zaniechanie podlega ograniczeniu zarówno od strony podmiotowej, jak i przedmiotowej. Ograniczenia podmiotowe normy statuującej obowiązek gwaranta sprowadzają się do stwierdzenia, że odpowiedzialności karnej za przestępstwo skutkowe popełnione przez zaniechanie będzie podlegał jedynie ten podmiot, na którym ciążył prawny, szczególny obowiązek zapobiegnięcia skutkowi, czyli tzw. gwarant nienastąpienia skutku[17]. Ograniczenia przedmiotowe służą przede wszystkim ustaleniu wymaganych w danej sytuacji od podmiotu reguł ostrożności w postępowaniu z określonym dobrem prawnym. Reguły ostrożności to określone normy postępowania z takim dobrem, które maja charakter techniczny i jako oparte na wiedzy i doświadczeniu nakazują w określonych sytuacjach podjęcie określonych ruchów w celu zapobiegnięcia określonemu skutkowi[18]. Ograniczenia przedmiotowe zawężają odpowiedzialność ze względu na rodzaj dóbr, które gwarant zobowiązany jest chronić i ze względu na charakter grożącego dobru niebezpieczeństwa[19]. Obiektywne przypisanie skutku przy przestępstwach materialnych z zaniechania charakteryzuje się odmiennością w stosunku do przestępstw materialnych z działania[20]. Odrzucając koncepcję przyczynowości zaniechania[21], należy przyjąć, że przypisanie skutku w przypadku zaniechania może zostać oparte wyłącznie na płaszczyźnie normatywnej, inaczej powiązaniu normatywnym[22].

Koniecznym warunkiem przyjęcia odpowiedzialności określonego pod-

---

[17] J. M a j e w s k i, *Prawnokarne przypisanie skutku przy zaniechaniu*, Kraków 1997, s. 62 i n.; A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, tezy 11, 13, 14 do art. 2.

[18] A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, teza 9 do art. 2.

[19] *Ibid.*, teza 12 i 19 do art. 2.

[20] Zob. w szczególności J. M a j e w s k i, *op. cit.*, s. 68 i n.; A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, teza 2 do art. 2. Chodzi w szczególności o fakt, iż przypisanie skutku przy przestępstwach materialnych popełnionych przez zaniechanie nie wymaga ustalenia powiązania przyczynowego, którego ustalenie jest elementem koniecznym w przypadku przestępstw materialnych popełnionych z działania, a jedynie powiązania normatywnego pomiędzy naruszeniem reguł ostrożności a skutkiem, który wystąpił.

[21] A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, teza 2, 7 i 8 do art. 2; W. W o l t e r, *O tzw. przyczynowości zaniechania*, PiP 1954, z. 10/11; J. M a j e w s k i, *op. cit.*, s. 56 i n.; A. Z o l l, *Odpowiedzialność...*, *op. cit.*, s. 46.

[22] A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, teza 2 i 8 do art. 2; A. Z o l l, *Odpowiedzialność...*, *op. cit.*, s. 48; W. W o l t e r, *O tzw. przyczynowości zaniechania*, PiP 1954, z. 10/11, s. 521 i n. J. M a j e w s k i, *op. cit.*, s. 48 i n.

miotu za skutek przestępny powstały przez zaniechanie jest ustalenie, iż (i) rzeczony podmiot jest gwarantem nienastąpienia skutku, tzn. spoczywa na podmiocie prawny, szczególny obowiązek zapobiegnięcia skutkowi, (ii) doszło do aktualizacji obowiązku gwaranta, (iii) doszło do zaniechania przez gwaranta wymaganych od niego w danych okolicznościach działań, mogących obiektywnie rzecz biorąc zapobiec wystąpieniu skutku o charakterze przestępnym, (iv) że zaniechanie owych wymaganych działań było jednocześnie naruszeniem reguł ostrożności, czyli reguł postępowania z danym dobrem, które to reguły miały za zadanie chronić określone dobro prawne przed wystąpieniem skutku przestępnego na tej drodze, na której skutek się zrealizował, (v) niezbędne jest ustalenie, że to właśnie zaniechanie określonego w danych okolicznościach działania, do którego podjęcia podmiot był zobowiązany, zapobiegłoby wystąpieniu skutku przestępnego. Poza powyższym, gwarant musi mieć obiektywną możliwość przewidzenia wystąpienia skutku oraz musi posiadać możliwość podjęcia — ocenianą *ex ante* — wymaganego od gwaranta działania.

Zgodnie z tym, co już napisano powyżej, możliwość odpowiedzialności na gruncie art. 2 k.k. może dotyczyć jedynie gwaranta nienastąpienia skutku. Ustalenie źródła takiego obowiązku nie jest częstokroć oczywiste. Obowiązek statuujący pozycję gwaranta musi mieć charakter prawny. W przypadku ustalenia źródła obowiązku odpowiedzialności prawnokarnej administratora danych za spowodowanie skutku przez procesora jest ewidentne. W art. 31 ust. 4 o.d.os. daje bowiem wyraźną podstawę do przyjęcia, iż administrator danych w przypadku powierzenia przetwarzania danych procesorowi nadal pozostaje odpowiedzialny za zgodne z ustawą o ochronie danych osobowych przetwarzanie danych osobowych: „w przypadkach, o których mowa w ust. 1–3[23], odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzane danych niezgodnie z tą umową". Powyższy artykuł statuuje prawny obowiązek po stronie administratora pieczy nad zgodnym z prawem przetwarzaniem da-

[23] Art. 31 ust. 1 o.d.os. stanowi „Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych". Ust. 2: „Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Ust. 3: „Podmiot, o którym mowa w ust.1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36–39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych".

nych osobowych przez procesora, któremu powierzył on ich przetwarzanie. Prawny obowiązek musi posiadać charakter szczególny, tzn. norma prawna nakłada go nie na każdego, lecz na osoby charakteryzujące się wskazanymi przez nią cechami, wyróżniającymi je z uwagi na stosunek do dobra chronionego normą prawną[24]. Taki szczególny obowiązek spoczywa na konkretnym administratorze powierzającym przetwarzanie danych określonemu procesorowi. Oczywiście dyspozycja cytowanego powyżej przepisu *in fine* nie wyklucza odpowiedzialności samego procesora za niezgodne z prawem działania.

Treść obowiązku gwaranta (administratora danych) w przypadku powierzenia przetwarzania danych, sprowadza się do podjęcia takich działań przez administratora, aby doprowadziły one do zneutralizowania niebezpieczeństwa, ewentualnie jego zmniejszenia grożącego dobru prawnemu, jakim w tym przypadku jest poufność danych osobowych w granicach wyznaczonych przez zasadę celowości i zasadę bezpieczeństwa danych[25]. Inaczej mówiąc administrator danych powinien podjąć takie działania, aby nie doszło do niedozwolonego przetwarzania (wywołania skutku w postaci udostępnienia danych osobom nieupoważnionym) danych osobowych przez procesora. Należy pamiętać, iż nie chodzi tutaj o zapewnienie całkowitego bezpieczeństwa, ale raczej o takie, które jest na tyle poważne, że należałoby je wziąć pod uwagę w określonym stanie faktycznym. Norma statuująca obowiązki gwaranta nie nakazuje jakiegoś postępowania samego przez się, jakiegoś postępowania w sposób formalny, ale nakazuje spowodowanie określonego stanu rzeczy — zapewnienie stanu bezpieczeństwa dobru prawnemu, nad którym gwarant ma pieczę[26]. Takim działaniom musi towarzyszyć wiedza adresata normy o tym, co powinien czynić, aby zapewnić bezpieczeństwo chronionemu dobru. W kontekście odpowiedzialności administratora danych nie ulega wątpliwości, iż jednym z podstawowych działań, mającym za zadanie właściwie zabezpieczyć dane osobowe przed ich niewłaściwym udostępnieniem, jest zawarcie przez administratora umowy powierzenia przetwarzania danych, która nakładając na procesora zobowiązania zgodnego z prawem przetwarzania danych, świadczy jednocześnie, iż administrator dokłada należytej staranności, by zabezpieczyć w odpowiedni sposób procesy przetwarzania danych. Celem

---

[24] A. Zoll, w: G. Bogdan, Z. Ćwiąkalski, P. Kardas [i in.], *op. cit.*, s. 81 i n.
[25] J. Barta, P. Fajgielski, R. Markiewicz, *op. cit.*, s. 737; A. Adamski, *op. cit.*, s. 163.
[26] J. Majewski, *op. cit.*, s. 74.

— jak słusznie podkreśla się w literaturze — nałożenia na administratora danych obowiązku zawarcia umowy powierzenia przetwarzania danych, jest zapobieżenie sytuacjom, w których powierzenie przez administratora danych procesorowi prowadziłoby do osłabienia ich ochrony oraz mogłoby uszczuplać uprawnienia osób, których dane dotyczą[27]. Zawarcie takiej umowy wydaje się być swoistą regułą ostrożnościową, regułą techniczną, której zachowanie ma wyeliminować lub relatywnie zmniejszyć zagrożenie niezgodnego z prawem przetwarzania danych osobowych, w tym ich udostępnienia podmiotom nieupoważnionym. Umowa zgodnie z art. 31 ust. 1 powinna być zawarta w formie pisemnej[28], powinna określać dozwolony cel i zakres przetwarzania powierzonych danych oraz zobowiązywać procesora do odpowiedniego zabezpieczenia przetwarzanych danych. Uznaje się, że są to *essentialia negotii* umowy powierzenia przetwarzania danych, bez których określenia zawarta umowa nie może być traktowana jako umowa powierzenia przetwarzania danych. Uznanie, iż mimo zawarcia umowy nie doszło do zawarcia umowy powierzenia przetwarzania danych prowadzi do bezpośredniego wniosku, iż jeden z głównych obowiązków spoczywających na administratorze danych powierzającym przetwarzania danych nie został przez niego dopełniony[29]. Administrator danych jest zobowiązany, co do zasady, do przetwarzania danych osobowych jedynie w celach, dla których je pozyskał i nie jest uprawniony do ich dalszego przetwarzania wykraczającego poza pierwotny cel przetwarzania danych osobowych. Obowiązek dochowania celu przetwarzania danych osobowych przez samego administratora oraz podmioty, którym powierza on przetwarzania danych osobowych został wyraźnie określony art. 26 ust. 1 pkt 2 o.d.os. W związku z powyższym słusznie można założyć, iż z ustawy o ochronie danych osobowych wynika obowiązek zawierania stosunków powierzenia przetwarza-

---

[27] J. B a r t a, P. F a j g i e l s k i, R. M a r k i e w i c z, *op. cit.*, s. 614.

[28] Z punktu widzenia prawa cywilnego umowa o powierzenie przetwarzania danych zawarta w formie ustnej będzie ważna. Ustawa bowiem nie zastrzega formy pisemnej pod rygorem jej nieważności. Niemniej jednak, w przypadku zawarcia umowy w formie ustnej byłoby bardzo trudno udowodnić administratorowi danych, iż umownie zobowiązał procesora do przetwarzania danych w taki sposób, aby nie naruszało to praw osób, których dane podlegają przetwarzaniu. Dodatkowo, należy pamiętać, iż przepisy ustawy o ochronie danych osobowych mają charakter przepisów administracyjnych, a więc proste przełożenie skuteczność zawarcia umowy np. w formie ustnej nie może być równoznaczne z realizacją wymogu zawarcia umowy we właściwej formie, tj. pisemnej, jaką nakłada na administratora danych art. 31 o.d.os.

[29] A. D r o z d, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2004, s. 197.

nia danych osobowych w taki sposób, aby administrator danych osobowych mógł zagwarantować poprawność przetwarzania danych osobowych przez procesora w zakresie celu przetwarzania[30]. Innymi słowy administrator może powierzyć przetwarzanie danych procesorowi tylko w tym celu, do jakiego jest sam umocowany. Podobnie rzecz się ma z zakresem przetwarzania danych osobowych. Zawarcie umowy precyzującej cel, zakres oraz nakładającej obowiązek zabezpieczenia danych jest realizacją obowiązku spoczywającego na administratorze jako gwarancie nienastąpienia skutku. Wydaje się, iż co do zasady, zawarcie umowy zobowiązującej podmiot do podejmowania określonych działań na danych osobowych jedynie w celu i zakresie wyznaczonym taką umową zabezpiecza przed odpowiedzialnością karną administratora danych za skutek. Gdyby bowiem procesor dokonał udostępnienia danych osobom nieupoważnionym wbrew umowie, wtedy trudno byłoby administratorowi, co do zasady, zarzucić naruszenie reguł ostrożności i w konsekwencji przekroczenie normy statuującej obowiązki gwaranta. W pewnych stanach faktycznych, wydaje się jednak, iż skutek w postaci udostępnienia danych mógłby zostać przypisany administratorowi nawet w przypadku zawarcia umowy powierzenia danych, np. przy świadomości gwaranta, że procesor nie spełnia warunków właściwego zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, np. pracodawca powierza przetwarzanie danych pracowników innemu podmiotowi zdając sobie sprawę, że taki podmiot nie jest w stanie ich należycie zabezpieczyć lub właściciel serwisu internetowego powierza przechowywanie treści hosting providerowi, w sytuacji, gdy ten ostatni nie spełnia warunków ich bezpiecznego przechowywania. W takiej sytuacji administrator narusza reguły ostrożności postępowania z określonym dobrem pomimo realizacji jednej z naczelnych reguł ostrożnościowych, mianowicie zawarcia umowy powierzenia danych. Nie ulega wątpliwości, iż administrator jako gwarant powinien dołożyć należytej staranności celem właściwego zabezpieczenia danych przed ich udostępnieniem, co powinno przejawiać się w pierwszej kolejności z właściwym zobowiązaniem procesora do zgodnego z prawem (podstawami przetwarzania) przetwarzania danych osobowych. Zawarcie samej umowy w przypadku powierzenia, choć jest elementem podstawowym, nie wyczerpuje obowiązków spoczywających na administratorze danych powierzającym dane do przetwarzania procesorowi.

Artykuł 31 ust. 3 o.d.os. statuuje po stronie procesora zobowiązanie do

---

[30] A. K r a s u s k i, D. S k o l i m o w s k a, *Dane osobowe w przedsiębiorstwie*, Warszawa 2007, s. 148.

realizacji wielu obowiązków mających zapewnić bezpieczeństwo przetwarzanych danych osobowych, w szczególności procesor powinien, jeszcze przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych opisane w art. 36–39 o.d.os., a więc m.in. wdrożyć środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do kategorii zagrożeń oraz kategorii danych objętych ochroną. W kolejności, procesor powinien prowadzić również dokumentację dotyczącą przetwarzania danych, czyli politykę bezpieczeństwa ochrony danych oraz instrukcję zarządzania systemem informatycznym, w którym przetwarza się dane osobowe, o ile, w ostatnim przypadku, dane przetwarzane są metodami informatycznymi. Poza powyższym, procesor jest zobowiązany do wyznaczenia administratora bezpieczeństwa informacji, dopuszczenia do przetwarzania danych osobowych jedynie osób upoważnionych, prowadzić ewidencję takich osób oraz sprawować kontrolę nad tym, jakie dane, przez kogo i kiedy zostały do zbioru wprowadzone. Inne obowiązki, które powinien spełnić administrator oraz procesor wynikają z aktów podustawowych[31]. Szeroki zakres obowiązków spoczywający na procesorze nie jest jednak tożsamy z zakresem obowiązków, któremu podlega administrator danych. Procesor nie jest zobowiązany, co do zasady, do rejestracji zbioru danych, choć taki obowiązek może w drodze umowy nałożyć na niego administrator danych. Procesor również nie musi dopełniać obowiązków informacyjnych względem osób, których dane dotyczą. Ten obowiązek spoczywa na administratorze danych. Oczywiście, w sytuacji, gdy procesor zbiera w imieniu administratora dane osobowe bezpośrednio od osób, których one dotyczą, umowa powierzenia danych powinna nałożyć na procesora dopełnienie takiegoż obowiązku, tym bardziej, że jego aktualizacja następuje przed rozpoczęciem zbierania danych[32].

W świetle powyższego nie można ograniczać roli administratora danych jako gwaranta li tylko do zawarcia umowy powierzenia przetwarzania danych, lecz należy ją utożsamiać również z dość szeroko pojętym obowiązkiem kontroli procesora, tj. czy wypełnia on obowiązki opisane powyżej. Obowiązek zabezpieczenia danych przez administratora trwa bowiem tak długo, jak względem danych określony podmiot pozostaje właśnie ich administratorem. Właściwie ułożone relacje na płaszczyźnie kontrakto-

---

[31] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dn. 29 IV 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. Nr 100, poz. 1024.

[32] A. D r o z d, *op. cit.*, s. 133.

wej poprzez zawarcie stosownej umowy przez administratora, pozwalają, w bardzo dużym zakresie ograniczyć jego potencjalną odpowiedzialność za skutek w postaci udostępnienia danych spowodowany przez procesora, lecz jej nie wykluczają. Innymi słowy na administratorze spoczywa obowiązek stałej kontroli procesów przetwarzania danych przez procesora. Gwarant, którym w tym przypadku jest administrator danych zobowiązany jest do racjonalnego wykorzystania wszystkich dostępnych metod i środków w celu odwrócenia grożącego dobru prawnemu ryzyka[33]. Ocena racjonalności zachowania się gwaranta powinna nastąpić poprzez porównanie z wzorcem racjonalnie działającego gwaranta, którym w tym przypadku byłby racjonalnie działający administrator danych[34]. Ustalenie przez administratora, że doszło do naruszeń np. zasad bezpieczeństwa przez procesora, powinno skutkować zobowiązaniem procesora do natychmiastowej poprawy stosowanych zabezpieczeń lub ich wdrożenia. Brak podjęcia określonych działań przez administratora względem procesora w sytuacji naruszenia zasad bezpieczeństwa przez tegoż ostatniego, może prowadzić do uznania, że to właśnie administrator narusza reguły ostrożności w postaci braku kontroli procesów przetwarzania danych przez procesora. Jeżeli w ocenie administratora przetwarzanie danych przez procesora niesie za sobą ryzyko zaniedbań w sferze zabezpieczenia danych, które może skutkować w dalszej kolejności ich udostępnieniem osobom nieupoważnionym, powinien on dokonać stosownych działań prowadzących bezpośrednio do wyeliminowania lub znacznego ograniczenia niebezpieczeństwa dla dobra prawnego, inaczej ryzyka wystąpienia skutku przestępnego. Słuszne wydaje się przyjęcie — znów powołując się na analogię wypracowanych konstrukcji odpowiedzialności za pracę w zespole — w podobnych sytuacjach tzw. zasady ograniczonego zaufania do innego członka zespołu, a więc że ów inny członek zespołu będzie postępował zgodnie z obiektywnymi regułami ostrożności tak długo, jak długo w jego zachowaniu nie wystąpią cechy wskazujące na to, że może on ten obowiązek naruszyć[35]. Innymi słowy, dopóki procesor swoim zachowaniem nie zdradza, że jego działania/zaniechania mogą zagrażać dobru prawnemu, tak długo specjalna aktywność ze strony administratora nie jest wymagana. W innym wypadku, gdyby skutek w postaci udostępnienia danych wystąpił, a był on obiektywnie dla administratora

[33] A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, teza 25 do art. 2.

[34] Szerzej na ten temat M. R o d z y n k i e w i c z, *Modelowanie pojęć w prawie karnym*, Kraków 1998, s. 87 i n.

[35] A. Z o l l, *Odpowiedzialność...*, *op. cit.*, s. 88.

danych przewidywalny (procesor podejmował/nie podejmował pewnych czynności, które obiektywnie wskazywały na możliwość spowodowania zagrożenia dla dobra prawnego), wtedy przypisanie mu tego skutku na płaszczyźnie art. 2 k.k. wydaje się być prawdopodobne[36]. Słuszne jest, posługując się pewnymi wnioskami przedstawionymi wcześniej w kontekście ustalenia odpowiedzialności za skutek w ramach pracy w zespole, przyjęcie, że na administratorze ciąży obowiązek właściwego zorganizowania przetwarzania danych osobowych, co powinno przejawiać się przede wszystkim we właściwym doborze podmiotu mającego przetwarzać takie dane (ocenie, czy procesor zapewnia właściwy poziom realizacji zadań, w tym zabezpieczenia danych przed ich udostępnieniem), zawarciem stosownej umowy właściwie określającej rolę procesora w procesie przetwarzania danych (tzn. w jakich celach i zakresie może on przetwarzać dane) oraz generalnego czuwania nad prawidłowym przetwarzaniem danych, w tym zapewnieniem im stosownego bezpieczeństwa. Niedochowanie powyższych reguł, które powinny być traktowane jako dyrektywy techniczne postępowania z dobrem prawnym, prowadziłoby do uznania, iż zostały naruszone określone reguły ostrożności przez administratora danych mające chronić dobro prawne przed niebezpieczeństwem. Dochowanie powyższych reguł, a więc, gdy doszło do należytego podziału wykonywania określonych czynności, tj. przetwarzanie danych zostało powierzone podmiotowi dającemu rękojmię właściwego przetwarzania danych, w tym ich bezpieczeństwa (procesor realizuje wszystkie obowiązki nałożone przez niego przepisami prawa), została zawarta umowa powierzenia przetwarzania danych właściwie określająca cel i zakres dozwolonego przetwarzania danych, która jednocześnie zobowiązuje procesora do odpowiedniego zabezpieczenia danych oraz nie występują inne okoliczności, które mogłyby świadczyć, że bezpieczeństwo danych jest zagrożone, wtedy odpowiedzialność administratora jako gwaranta za skutek, który pomimo przestrzegania powyższych reguł ostrożności wystąpił, byłaby bardzo trudna do przypisania. Innymi słowy działania administratora danych powinny być optymalne, tzn. takie, które w sposób najpełniejszy zabezpieczałyby dane osobowe przed ich udostępnieniem

---

[36] W związku z ryzykiem odpowiedzialności za skutek spowodowany przez procesora, administrator powinien zagwarantować w umowie możliwość przeprowadzania czynności kontrolnych. Natomiast w sytuacji, gdy procesor nie chce współpracować z administratorem danych, a ten ostatni ma uzasadnione podejrzenia niezgodnego z prawem przetwarzania powierzonych procesorowi danych, powinien poinformować o tym fakcie albo Generalnego Inspektora Ochrony Danych Osobowych, albo odpowiednie organy ścigania, o ile zachodzi podejrzenie popełnienia przestępstwa.

podmiotom nieupoważnionym. Przyjęcie, iż postępowanie administratora danych było w określonych warunkach optymalne (sytuacja oceniana *ex ante*) prowadzi do przyjęcia wniosku, że nie przekroczył on normy statuującej obowiązki gwaranta, jeżeli natomiast stwierdzimy, że postępowanie to nie było optymalne, to tym samym uznamy, że wspomniana norma prawna została przez administratora naruszona[37]. Warto również podkreślić, iż nie jest wystarczające podjęcie jakichkolwiek działań przez gwaranta, lecz działań racjonalnych, które w danej sytuacji zapewniają przeciwdziałanie wystąpieniu określonego skutku[38]. W sytuacji, w której pomimo nastąpienia przestępnego skutku w postaci udostępnienia danych osobom nieupoważnionym zachowanie administratora było zgodne z regułami ostrożności, nie może być mowy o naruszeniu normy statuującej obowiązki gwaranta. Trudno byłoby w takiej sytuacji administratorowi przypisać skutek przestępny w postaci udostępnienia danych podmiotom nieupoważnionym, który został bezpośrednio spowodowany przez procesora.

Nie można wykluczyć, iż w sytuacji powierzenia, to procesor, w zakresie zobowiązania umownego, mógłby stać się gwarantem nienastąpienia skutku przestępnego[39]. Przyjęcie roli gwaranta na podstawie umowy nie jest w tym zakresie kwestionowane[40]. W tym miejscu warto zauważyć, iż przestępny skutek w postaci udostępnienia danych może być rezultatem naruszenia reguł ostrożności jednocześnie przez administratora oraz procesora. W takiej sytuacji może pojawić się bardzo interesujące zagadnienie przypisywalności skutku, gdy do jego zaistnienia konieczne jest skumulowanie się bezprawnego zachowania się co najmniej dwóch osób, z których każde

---

[37] J. M a j e w s k i, *op. cit.*, s. 76.

[38] K. B u c h a ł a, A. Z o l l, *op. cit.*, s. 193.

[39] Zob. w szczególności postanowienie SN z 11 XII 2000 r., II KKN 438/2000, OSNKW 2001, nr 3/4, poz. 33. Na gruncie tegoż postanowienia, SN przyjął odpowiedzialność karną procesora za skutek w postaci udostępnienia danych podmiotom nieupoważnionym, w sytuacji gdy przekazał on je kolejnemu podmiotowi celem ich zniszczenia. Sąd Najwyższy zauważył: „[…] i nie można przyjąć, iżby przez przekazanie jej [makulatury — przyp. moje, G.K.] owym zakładom jako makulatury tajnej uwolnił się [oskarżony — przyp. moje, G.K.] automatycznie od odpowiedzialności karnej z art. 51 ustawy ochronie danych osobowych. To on bowiem w pierwszej kolejności był odpowiedzialny za ochronę danych zakresie określonym w tym przepisie, a samo przekazanie tych danych do zniszczenia innemu podmiotowi nie gwarantuje ich zniszczenia bez dostępu do danych osób nieupoważnionych, nie może oznaczać uwolnienia się obowiązanego do ochrony danych od odpowiedzialności za tę ochronę".

[40] A. Z o l l, w: G. B o g d a n, Z. Ć w i ą k a l s k i, P. K a r d a s [i in.], *op. cit.*, teza 20 do art. 2; G. R e j m a n, w: *Kodeks*..., *op. cit.*, teza 11 do art. 2; L. G a r d o c k i, *Prawo karne*, Warszawa 2001, s. 67.

będzie normatywnie powiązane ze skutkiem, tzw. kolizja odpowiedzialności za skutek[41].

Należy również zwrócić uwagę, że umowa powierzenia przetwarzania danych zabezpiecza nie tylko administratora danych przed przestępnymi działaniami procesora, lecz również chroni samego procesora przed zarzutem niezgodnego z prawem przetwarzania danych. Umowa bowiem precyzuje cel i zakres dozwolonego przetwarzania danych przez procesora. Tym samym, jeżeli procesor został umocowany umową do przetwarzania danych w zakresie/celu szerszym niż do tego miał prawo administrator, a fakt ten pozostał jedynie w sferze świadomości administratora, procesor nie będzie ponosił odpowiedzialności za niezgodne z prawem przetwarzanie danych. Jeżeli więc administrator danych dysponujący bazą danych osób, która faktycznie jest powierzona do przetwarzania procesorowi, zobowiązuje procesora do — na jego żądanie — sprzedaży (licencjonowania) bazy danych pomimo braku podstaw prawnych do takiego udostępniania np. braku zgód osób, których dane dotyczą, wtedy procesor będzie działał w ramach umocowania umownego i nie narazi się na odpowiedzialność karną za tego typu działania, chyba że w powyższej sytuacji można by procesorowi udowodnić realizację znamion współsprawstwa lub pomocnictwa do takiego czynu. Z powyższych względów zawarcie umowy powierzenia przetwarzania danych przede wszystkim zabezpiecza administratora danych, lecz również w pewnych sytuacjach zabezpiecza procesora przed potencjalną jego odpowiedzialnością.

By móc przypisać skutek administratorowi danych musi zachodzić również jego obiektywna możliwość przewidzenia. W sytuacji, gdy obiektywnie ujmując, mimo istnienia jakiegoś skonkretyzowanego niebezpieczeństwa dla dobra prawnego, kontekst sytuacyjny nie dostarcza odpowiedniego zakresu informacji, wystarczającego do jego rozpoznania, skierowany do gwaranta nakaz żadną miarą nie może być zrealizowany[42]. Oczywiście, nie chodzi w tym momencie o indywidualistycznie pojmowaną możliwość przewidzenia nastąpienia skutku odnoszoną do konkretnego administratora, lecz o taką obiektywną możliwość przewidzenia wystąpienia skutku, którą będziemy oceniali przez pryzmat wzorcowego (modelowego) administratora danych[43]. W sytuacji, gdy administrator danych podjął wszelkie niezbędne

---

[41] M. B i e l s k i, *Obiektywne przypisanie skutku przestępnego w przypadku kolizji odpowiedzialności za skutek*, PiP 2005, z. 10, s. 82.

[42] J. M a j e w s k i, *op. cit.*, s. 68.

[43] M. R o d z y n k i e w i c z, *op. cit.*, s. 120 i 135.

kroki dla zapobieżenia naruszeniu reguł postępowania dotyczących danych osobowych i obiektywnie rzecz biorąc możliwość przewidzenia wystąpienia skutku była wykluczona, a mimo wszystko taki skutek w postaci udostępnienia danych osobowych wystąpił, przypisanie go administratorowi nie będzie możliwe.

Administrator danych, aby móc mu przypisać skutek, musi również mieć możliwość podjęcia określonych działań mogących obiektywnie zapobiec wystąpieniu skutku przestępnego. Możliwość działania powinna zawsze być odnoszona do konkretnych okoliczności, w których przyszło działać administratorowi. Nie ulega wątpliwości, iż status administratora danych jako podmiotu decydującego o celach i środkach przetwarzania danych osobowych uprawnia go do podejmowania decyzji, co do przetwarzania danych. Do decyzji administratora danych jest zobowiązany stosować się każdorazowo procesor. Trudno sobie wyobrazić sytuację, w której administrator byłby pozbawiony jakiejkolwiek możliwości działania względem procesora w przypadku łamania przez tego ostatniego postanowień umowy powierzenia przetwarzania danych i/lub regulacji ustawowych lub wykonawczych do ustawy o ochronie danych osobowych[44].

Ostatnim warunkiem, który musi zaistnieć, by móc pociągnąć administratora danych do odpowiedzialności karnej jest ustalenie, że zachowaniu sprawcy można przypisać na płaszczyźnie normatywnej skutek. Inaczej mówiąc należy dowieźć, że zachodzi normatywne powiązanie pomiędzy skutkiem wywołanym przez procesora a zachowaniem administratora, polegającym na braku po jego stronie działań nakierowanych na usunięcie/istotne zmniejszenie grożącego dobru prawnemu niebezpieczeństwa. Ustalenie, iż w przypadku podjęcia przez administratora danych odpowiednich i stosownych do okoliczności działań prowadziłoby do wykluczenia wystąpienia skutku przestępnego, umożliwiałoby jego przypisanie administratorowi i w oparciu o konstrukcje art. 2 k.k. pociągnięcie administratora danych do odpowiedzialności karnej za ten skutek. Należy podkreślić, że nie chodzi tutaj bynajmniej, o takie założenie, iż ustawowo stypizowany skutek mógłby zostać przypisany sprawcy tylko wtedy, gdyby ustalenia prowadziły do przyjęcia, że wykonanie przez sprawcę nakazanego czynu, z pewnością lub z prawdopodobieństwem graniczącym z pewnością zapo-

[44] W szczególności chodzi tutaj o regulacje przewidziane rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dn. 29 IV 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, Dz.U. Nr 100, poz. 1024.

biegłoby urzeczywistnieniu się tego skutku. Wydaje się, że chodzi raczej o przyjęcie, iż przypisanie ustawowo stypizowanego skutku jest możliwe wtedy, gdy wykonanie czynu faktycznie zaniechanego poprawiałoby szanse uniknięcia skutku, inaczej w sposób znaczny zmniejszałoby ryzyko wystąpienia takiego skutku[45]. Na koniec warto również podkreślić, że nie można wykluczyć, iż nawet w przypadku naruszenia przez administratora normy statuującej obowiązki gwaranta poprzez naruszenie stosownych reguł ostrożności postępowania z dobrem, stypizowany skutek nie zostanie mu przypisany, gdyby doszło do ustalenia, że w analizowanym przypadku skutek wystąpiłby pomimo zrealizowania rzeczonej normy.

Należy pamiętać, iż pociągnięcie do odpowiedzialności karnej administratora danych nie wyklucza odpowiedzialności samego procesora za skutek przez niego wywołany[46].

Reasumując, przy założeniu, iż znamię czasownikowe „udostępniać" typu czynu zabronionego określonego w art. 51 ust. 1 o.d.os. konstytuuje typ przestępstwa materialnego i przy jednoczesnym spełnieniu wszystkich przesłanek przypisania odpowiedzialności za przestępstwo materialne popełnione przez zaniechanie, istnieje możliwość pociągnięcia do prawnokarnej odpowiedzialności administratora danych — na gruncie art. 2 k.k. — za wywołanie skutku w postaci przestępnego udostępnienia danych przez procesora, któremu administrator powierzył przetwarzanie danych.

---

[45] K. B u c h a ł a, A. Z o l l, *op. cit.*, s. 188; szerzej na ten temat J. M a j e w s k i, *op. cit.*, s. 88 i n.

[46] Zob. w szczególności orzeczenie SN z 11 XII 2000 r., II KKN 438/00, OSNKW 2001, nr 3/4, poz. 33; B. K u r z ę p a, *op. cit.*, s. 47.