Maciej SZMIT

Wybrane zagadnienia OPINIOWANIA sądowo-informatycznego

Maciej SZMIT

Wybrane zagadnienia O P I N I O W A N I A sądowo-informatycznego

EUROPEAN ASSOCIATION for SECURITY
KRAKÓW 2014

ISBN 978-83-61645-10-8

Recenzenci:

dr hab. Jacek Dworzecki, profesor Wyższej Szkoły Policji w Szczytnie
dr hab. Leszek Korzeniowski, profesor Akademii Wychowania Fizycznego w Krakowie
plk. doc. PaedDr. Samuel Uhrin, CSc.
- Akadémia Policajného zboru, Bratislava (Slovensko)
- profesor Akademii Pomorskiej w Słupsku
dr Andrzej Niemiec

Korekta: Magdalena Kopacz

Wydawca:
EUROPEAN ASSOCIATION for SECURITY
31-571 Kraków, al. Jana Pawła II 78 (AWF, IV, 317)
e-mail: lfk@eas.info.pl
http://www.eas.info.pl

Druk i oprawa:
Elpil
08-110 Siedlce, ul. Artyleryjska 11
tel. 25 643 65 51
e-mail: info@elpil.com.pl

Spis treści

Wstęp

Rozwój techniki (w tym „wysokich technik" telekomunikacji i przetwarzania informacji) oraz ich powszechne zastosowanie w życiu społecznym i gospodarczym sprawia, że zarówno w praktyce gospodarczej, jak i w administracji państwowej i w wymiarze sprawiedliwości coraz częściej pojawia się potrzeba wykorzystania biegłych – osób służących odpowiednim organom swoją wiedzą i fachowymi umiejętnościami. Rola biegłych we współczesnym postępowaniu sądowym jest trudna do przecenienia, jednocześnie nie cieszą się oni – ogólnie rzecz ujmując – najlepszą opinią. Zarówno informacje prasowe, jak i literatura fachowa, poruszając tematykę biegłych, często pokazują przykłady rażących błędów, czy wręcz patologii w opiniowaniu[1].

[1] Dotyczy to w zasadzie biegłych wszystkich specjalności. Dla przykładu kilka cytatów:

- ✓ „Zegarek o wartości ok. 20 000 zł biegły wycenił na kwotę 9660 zł (…). Biegły wyjaśnił, że zegarek wycenia drugi raz w życiu, jest bowiem biegłym od wyceny nieruchomości oraz, że przyjął założenie, że zegarek jest kradziony" (zob. A. Suchecka-Tarnacka: *Biegły sądowy a prawidłowy wynik postępowania sądowego*, http://www.rozwiązywaniesporów.pl/2013/12/20/biegly-sadowy-a-prawidlowy-wynik-postepowania-sadowego);
- ✓ „Sekcję zwłok ofiary śmiertelnego pobicia siekierą zlecono lekarzowi specjaliście anestezjologii. W trakcie sekcji biegły doszedł jednak do wniosku, iż nie poradzi sobie z opisem licznych ran rąbanych na głowie (...). Z własnej więc inicjatywy odciął głowę, która została dostarczona bez postanowienia prokuratury do naszego Zakładu w wiaderku przez pracownika firmy pogrzebowej (...). Problem nie do rozstrzygnięcia tyczył poprzedzającego zadanie ran głowy dławienia, gdyż z powodu jej odcięcia na wysokości połowy szyi badanie tego rejonu zostało uniemożliwione" (zob. J. Kunz: *Błąd w opiniach sądowo-lekarskich w sprawach przestępstw przeciwko zdrowiu i życiu*, Katedra Medycyny Sądowej Collegium Medicum UJ, Kraków 1999, s. 36);
- ✓ „W normie z 1976 r., na którą powołuje się biegły, istnieją informacje, których nie sposób przełożyć na współczesne parkieciarstwo. Normalizacja za czasów PRL-u miała charakter normalizacji państwowej, a Polskie Normy (PN) oraz normy branżowe (BN) były obowiązkowymi normami i pełniły rolę przepisów. Jednak od 1994 r.

Już samo to jest wystarczającym usprawiedliwieniem dla podjęcia tematyki opiniowania sądowego z zakresu informatyki, tym bardziej że wśród stosunkowo wielu pozycji poświęconych metodykom pracy biegłych[2] i poszczególnym technikom kryminalistycznym[3], stosunkowo mało jest materiału dotyczącego opiniowania przez biegłych informatyków, wydanego w języku polskim i odnoszącego się do realiów polskiego systemu prawnego[4].

---

wszystkie normy branżowe przestały obowiązywać i zostały przeniesione do archiwum. O takich uwarunkowaniach prawnych biegły powinien wiedzieć i w związku z tym nie powinien opierać się na normatywach, które nie istnieją" (zob. M. Kuczyńska-Cichocka: *Biegły, ale czy na pewno specjalista*, „Profesjonalny parkiet" 3/2008), http://terazmedia.nazwa.pl/pparkiet/index.php?option=com_content&task=view&id=36).

Opinie informatyczne nie odbiegają od tego smutnego standardu:

- ✓ „Miałem okazję wysłuchać wykładu biegłego sądowego z dziedziny informatyki. Przyznam, że włos mi się zjeżył na głowie. Pan biegły opisał sposób, w jaki – na zlecenie prokuratora – zabezpieczał dowody, w toczącym się przed sądem postępowaniu (...). Uczestnicy konferencji usłyszeli anegdotę, jak to kiedyś swoim śrubokrętem, rzeczony biegły doprowadził do spalenia twardego dysku no i dowody przestępstwa przepadły" (zob. P. Waglowski: *And justice for all dot com*, http://prawo.vagla.pl/node/2858).

Jako patologiczne należy ocenić również sytuacje powoływania nadmiarowej liczby biegłych. W swojej pracy Ryszard Zahorski wspomina o trwającym 9 lat postępowaniu sądowym przez które przewinęło się dziewięciu biegłych i rzeczoznawców (R. Zahorski: *Metodyka pracy biegłego sądowego. Rekonstrukcja wypadku drogowego*, Difin, Warszawa 2010, s. 30).

[2] Np. K. Eichstaedt, P. Gałecki, A. Depko: *Metodyka pracy biegłego psychiatry, psychologa oraz seksuologa w sprawach karnych*, LexisNexis, Warszawa 2012; J. Wójcikiewicz: *Ekspertyza sądowa*, Zakamycze, Kraków 2002; R. Zachorski: *Metodyka pracy...*, op. cit.

[3] Np. T. Hanausek: *Kryminalistyka – zarys wykładu*, Zakamycze, Kraków 2005; S. Kozdrowski: *Kryminalistyka. Wybrane zagadnienia*, NWSP, Białystok 2012; E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka – czyli rzecz o metodach śledczych*, WAiP, Warszawa 2008; J. Wójcikiewicz: *Temida nad mikroskopem*, TNOiK, Toruń 2009.

[4] Szczególnie cennym wyjątkiem jest seria materiałów konferencji Techniczne Aspekty Przestępczości Teleinformatycznej organizowanej rokrocznie przez Wyższą Szkołę Policji w Szczytnie (zob. np.: A. Misiuk, P. Ciszek, J. Kosiński: *Przestępczość teleinformatyczna: VI seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2003; J. Kosiński: *Przestępczość teleinformatyczna: VII seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2004; J. Kosiński: *Przestępczość teleinformatyczna: VIII seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2005; J. Kosiński: *Przestępczość teleinformatyczna: IX seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji,

Nie można niestety zaprzeczyć, że i wśród opinii biegłych informatyków zdarzają się – i to zbyt często – opinie o rażąco niskiej jakości merytorycznej, jak również opinie budzące wątpliwości formalne. Niska jakość opinii, jak również zła współpraca biegłych z organami wymiaru sprawiedliwości, są jednymi z powodów problemów w pracy sądów i prokuratur prowadzących m.in. do zatorów w dynamice prowadzenia postępowań jurysdykcyjnych, co w konsekwencji przekłada się pejoratywnie na jakość życia i bezpieczeństwo państwa.

Celem przeprowadzonej przez autora analizy zagadnień opiniowania sądowo-informatycznego jest uporządkowanie pewnych kwestii związanych z występowaniem informatyków w roli biegłych sądowych, mających wpływ na pojawiające się niskie oceny tej pracy oraz wypracowanie wniosków zmierzających do poprawy tej jakości.

Autor ma nadzieję, że monografia, w chociażby niewielkim stopniu, wypełni lukę na krajowym rynku wydawniczym, w zakresie poruszanej problematyki i stanowić będzie zachętę do podjęcia dalszych prac z tego zakresu.

Przepisy o biegłych są rozproszone w kilkudziesięciu różnych aktach prawnych; sposób wykonywania przez biegłych swoich obowiązków zależy od rodzaju postępowania, w którym występują. Inne zasady regulują bowiem pracę biegłego w postępowaniu karnym (a w jego ramach inaczej wygląda praca biegłego w postępowaniu przygotowawczym, a inaczej w postępowaniu sądowym w sprawie karnej), inne – w postępowaniu cywilnym, a jeszcze inne – w postępowaniu administracyjnym. Warto podkreślić, że oprócz samych przepisów dużą rolę odgrywa ich wykładnia i praktyka

Szczytno 2006; J. Kosiński: *Przestępczość teleinformatyczna: X seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2007; J. Kosiński, J. Szafrański: *Przestępczość teleinformatyczna: XI seminarium naukowe: materiały seminaryjne*, pod red. J. Szafrańskiego, Wyższa Szkoła Policji, Szczytno 2008; J. Kosiński: *Przestępczość teleinformatyczna: XII seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2009. Z innych prac poświęconych zagadnieniom informatyki sądowej czy śledczej można wymienić pozycje: P. Frankowski: *Komputerowi detektywi. 111 porad*, Mikom, Warszawa 2005 i M. Szmit, A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec: *Elementy Informatyki Sądowej*, Polskie Towarzystwo Informatyczne, Warszawa 2011).

orzecznicza[5], a także praktyka współpracy organów wymiaru sprawiedliwości z biegłymi. Stąd też osoba powołana do pełnienia funkcji biegłego może mieć problem z jej formalnym aspektem. W praktyce opiniodawczej można też niejednokrotnie spotkać się z sytuacjami niepożądanymi, w tym błędami i pomyłkami ze strony zarówno biegłych, jak i wymiaru sprawiedliwości. Z tego powodu w monografii znalazły się fragmenty poświęcone takim sytuacjom jak: kwestie błędów w pytaniach do biegłych, kontaminacji materiału dowodowego, czy problemów z tzw. nielegalnym oprogramowaniem.

Autor serdecznie dziękuje P.T. Recenzentom za cenne merytoryczne uwagi, bez których powstanie tej pracy w jej obecnym kształcie nie byłoby możliwe.

[5] Stąd w monografii stosunkowo liczne cytaty z orzeczeń sądowych, przy czym należy pamiętać, że w przeważającej większości przypadków – nie są wiążące dla innych sądów, jakkolwiek tworzą pewną praktykę orzeczniczą.

1 Metodologiczne uwarunkowania roli opiniodawczej

Jednym z zadań dyscyplin stosowanych jest pełnienie roli opiniodawczej, czyli wydawanie przez przedstawicieli danej dyscypliny ekspertyz i opinii. Szczególne znaczenie, z uwagi na stopień sformalizowania i stopień związanej z nimi odpowiedzialności prawnej i moralnej, mają opinie wydawane na potrzeby administracji państwowej (opinie w postępowaniach administracyjnych) i wymiaru sprawiedliwości – opinie sądowe[6].

1.1 Działalność opiniodawcza a badania naukowe

Tradycyjnie wyróżnia się cztery podstawowe funkcje nauki[7]:

- ✓ deskryptywną (opisywanie rzeczywistości, odpowiedź na pytania: „jak jest", „jaki jest stan" itp.);
- ✓ eksplanacyjną (wyjaśnianie rzeczywistości, odpowiedź na pytania: „dlaczego", „z jakiego powodu" itp.);
- ✓ predykcyjną[8] (przewidywanie, wnioskowanie poza próbę, odpowiedź na pytanie: „jaki będzie dalszy przebieg zdarzeń");
- ✓ ewaluacyjną[9] (ocenianie)

[6] Ściśle rzecz ujmując opinie wykonywane na zlecenie organów prowadzących postępowanie przygotowawcze (np. prokuratur) bądź sądów.

[7] Por. np.: B.R. Kuc: *Funkcje nauki. Wstęp do metodologii. Nauka nie jest grą*, Wydawnictwo PTM, Warszawa 2012; L.F. Korzeniowski: *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2012, s. 44 i nast.

[8] W dalszej części pracy omówiono rozróżnienie pomiędzy diagnozą, prognozą i retrognozą. Pojęcie „funkcja predykcyjna" jest tutaj rozumiane tak, że nauka umożliwia prowadzenie rozważań dotyczących przyszłych lub przeszłych zachowań przedmiotu badania poprzez ekstrapolację poznanych reguł rządzących tymi zachowaniami poza dostępną do badania próbę.

[9] Niekiedy mówi się o funkcji aksjologicznej (wartościującej). Ewaluacja oznacza dosłownie „określenie wartości czegoś", szerzej używa się tego terminu na określenie systematycznego

oraz – niejako dodatkowo – funkcję pragmatyczną (instrumentalną, odpowiedź na pytanie: „co należy zrobić, aby było tak")[10]. Poszczególne funkcje nauki realizowane są w ramach badań naukowych oraz ogłaszania ich wyników[11]. Badaniem naukowym *sensu stricto* jest badanie realizujące co najmniej jedną z funkcji:

- ✓ teoretyczną, polegającą na konfrontowaniu aktualnie funkcjonujących teorii, ich korygowaniu oraz próbie konstruowania na ich podstawie nowych praw (teorii) naukowych;
- ✓ metodologiczną, polegającą na rozwijaniu instrumentarium badawczego przy tworzeniu śmiałych hipotez, ich empiryczną weryfikację, doszukiwania się istotnych zmiennych i ich wskaźników, a także na analizie tych zmiennych oraz ustalaniu związku i zależności w badanych zjawiskach, procesach i strukturach;
- ✓ praktyczną, polegającą na budowie modeli weryfikowanych empirycznie i w konsekwencji wdrażanych do praktyki[12].

Stosowanie metod nowatorskich jest – o czym jeszcze będzie dalej mowa – w opiniowaniu sądowym, co do zasady, niedopuszczalne, natomiast wspomaganie roli opiniodawczej jest jednym z zadań dyscyplin stosowanych[13], a jej pełnienie (wydawanie opinii i ekspertyz) – zadaniem ich przedstawicieli[14].

Proces prowadzenia dowodu z opinii biegłego podlega pewnym uwarunkowaniom, zarówno metodologicznym, jak i formalnoprawnym. Część

procesu oceny wartości cech przedmiotu badania z zastosowaniem określonych kryteriów tejże oceny.

[10] Nie jest konieczne, aby każde badanie naukowe realizowało wszystkie funkcje nauki. I tak np. badania o charakterze czysto poznawczym realizujące funkcję deskryptywną (opisową) mogą być w ogóle pozbawione elementów teoretycznych, niemniej dyscyplina naukowa, aby mogła nią być musi spełniać więcej niż jedną z wymienionych funkcji.

[11] Por. np. J. Bocheński: *Autonomia Uniwersytetu* [w:] *Sens życia i inne eseje*, PHILED, Kraków 1993, s. 60–72.

[12] Za: J. Apanowicz: *Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania*, WSAiB, Gdynia 2000, s. 20–21.

[13] Podobnie jak zadaniem medycyny jest m.in. określenie metodologicznych zasad prowadzenia badań lekarskich, czy jak zadaniem nauk technicznych jest np. opracowywanie poprawnych metodologicznie metod pomiarów technicznych parametrów konstrukcji inżynierskich.

[14] Stąd też na listach biegłych można znaleźć stosunkowo często pracowników uczelni, instytutów badawczych czy jednostek badawczo-rozwojowych.

z tych uwarunkowań jest identyczna z uwarunkowaniami dotyczącymi dowodu naukowego, część zaś jest w stosunku do niego bardziej restrykcyjna[15] – zostały one omówione bliżej w rozdziale dotyczącym dopuszczalności metod i narzędzi badawczych.

1.2 Interpretacja wartości diagnostycznej badania a metodyki pracy biegłego

W odniesieniu do zagadnień dotyczących metodologii naukowej, istotnych z punktu widzenia opiniowania, należy przede wszystkim poruszyć temat tworzenia przez naukowców dla biegłych (oraz dla sądów) zaleceń i kryteriów metodologicznych, w oparciu o które biegli później wydają opinie sądowe. Warto wiedzieć, że część z tego rodzaju kryteriów jest tworzona w sposób arbitralny. Dla przykładu w większości krajów europejskich, w tym w Polsce, w badaniach daktyloskopijnych bada się cechy identyfikacyjne obrazów linii papilarnych (minucje) przyjmując arbitralnie, że obecność kilku lub kilkunastu identycznych wariantów cech[16] w materiale kwestionowanym i porównawczym wystarcza do pewnego określenia tożsamości. Jest to tzw. standard numeryczny (doświadczalny).

Inne podejście (tzw. standard holistyczny lub ekspercki) obowiązuje w Stanach Zjednoczonych, Wielkiej Brytanii oraz krajach skandynawskich, gdzie opinię wydaje ekspert w oparciu o całościową ocenę materiału badawczego[17]. Przy przyjęciu standardu numerycznego, ustalenie liczby cech

[15] Jak już wspomniano, nie jest np. dopuszczalne stosowanie w opiniowaniu sądowym metod nowatorskich, ponadto istnieją zakazy dowodowe uniemożliwiające np. stosowanie hipnozy albo środków chemicznych lub technicznych wpływających na procesy psychiczne osoby przesłuchiwanej albo mających na celu kontrolę niewiadomych reakcji jej organizmu w związku z przesłuchaniem (art. 171 § 5 ust. 2 KPK).

[16] W różnych krajach od 8 do 17 cech wspólnych (przy czym liczba minucji może być mniejsza w przypadku wariantów rzadziej występujących). W Polsce przyjmuje się liczbę 12 minucji.

[17] Szczegółowe informacje na temat obu standardów i sporów pomiędzy ich zwolennikami zawiera artykuł J. Moszczyński: *Standardy identyfikacji daktyloskopijnej*, „Problemy Kryminalistyki" Nr 261/2008, s. 14–21. Na szczególną uwagę zasługuje przytoczony w nim tekst rezolucji 28 ekspertów daktyloskopii (z Australii, Francji, Holandii, Izraela, Nowej Zelandii, Szwajcarii, Szwecji, USA, Węgier i Wielkiej Brytanii) uczestniczących w międzynarodowym seminarium poświęconym ujawnianiu i identyfikacji śladów linii papilarnych w Ne'urim (Izrael) w 1995 r., którzy

potrzebnej do identyfikacji osoby opiera się zazwyczaj na – mniej lub bardziej skomplikowanych – obliczeniach statystycznych. W najprostszym przypadku znając liczbę i prawdopodobieństwo wystąpienia poszczególnych wariantów danych cech w populacji oraz zakładając niezależność występowania poszczególnych wariantów poszczególnych cech można obliczyć prawdopodobieństwo wystąpienia danego zestawu wariantów cech korzystając z klasycznego wzoru Bayesa na prawdopodobieństwo całkowite (prawdopodobieństwo *a posteriori*)[18], postępowanie to jest odpowiednio modyfikowane dla bardziej złożonych rozkładów prawdopodobieństwa apriorycznego.

O ile oczywiście nie można mieć wątpliwości co do poprawności samego wzoru Bayesa i obliczonego w ten sposób prawdopodobieństwa *a posteriori*, to już przyjęcie wartości granicznej, od której biegły twierdzić będzie, że wynik badania diagnostycznego jest pozytywny, jest decyzją arbitralną, zaś tak duże rozbieżności dla różnych krajów mogą budzić uzasadnione wątpliwości metodologiczne: liczba zgodnych wariantów cech wystarczających do uznania materiału kwestionowanego za zgodny z porównawczym w jednym kraju może być niewystarczająca do takiego uznania w innym; przy rozrzucie od 8 do 17 cech może okazać się, że nawet dwukrotnie większa liczba zgodności niż stwierdzona w wyniku badania nie byłaby wystarczająca do ustalenia zgodności według standardów obowiązujących w innym kraju. Tradycyjnie jednak wnioski z opinii daktyloskopijnej wyrażane są w sposób stanowczy, co zresztą jest przedmiotem krytyki w literaturze[19].

Z drugiej strony „standard holistyczny" również nie chroni przed możliwą skłonnością eksperta do sformułowania wniosków o nadmiernym

jednomyślnie stwierdzili, że brak jest naukowych podstaw do wymagania, aby w celu dokonania pozytywnej identyfikacji w dwóch obrazach (porównywanego śladu i odbitki) istniała z góry określona, minimalna liczba cech charakterystycznych linii papilarnych.

[18] W taki też sposób pierwotnie obliczono liczbę 12 minucji dla potrzeb daktyloskopii.

[19] Zob. E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka*…, op. cit., s. 332; J. Moszczyński: *Standardy*…, op. cit.; J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 94 i 118.

(lub niedoszacowanym) stopniu kategoryczności. Tam, gdzie jest to możliwe, wskazane jest podanie w opinii informacji o swoistości[20] i czułości[21] testu diagnostycznego[22], jak również wartości liczbowych prawdopodobieństwa *a posteriori* wraz z jego interpretacją. Takie podejście jest stosowane np. przy genetycznych badaniach identyfikacyjnych z wykorzystaniem DNA[23], gdzie jako wynik badania podaje się zazwyczaj iloraz wiarygodności („szansa ustalenia danej zgodności, jeżeli to nie podejrzany, a przypadkowa osoba pozostawiła ślad na miejscu zdarzenia wynosi 0,1%"[24]). Interpretacja tego ilorazu może nie być oczywista: w literaturze przedmiotu omawia się dwa błędy interpretacyjne zwane odpowiednio „sofizmatem prokuratora" i „sofizmatem adwokata"[25]. Sofizmat prokuratora polega na zinterpretowaniu powyższego zdania w ten sposób, że prawdopodobieństwo, że podejrzany jest winien wynosi 99,9% (jest więc niemal pewne), co jest oczywistym nadużyciem (szansa winy *a posteriori* powinna być liczona jako iloraz szansy winy *a priori* i ilorazu wiarygodności dowodu). Odwróceniem tego toku rozumowania jest sofizmat adwokata: jeśli iloraz wiarygodności dowodu wynoszący 0,1% miałby być jedynym czynnikiem przesądzającym o winie, to należałoby skazać za to przestępstwo co tysięczną osobę (a więc np. w milionowym mieście – tysiąc osób).

[20] Swoistość (specyficzność) testu diagnostycznego jest stosunkiem wyników prawdziwie ujemnych do sumy prawdziwie ujemnych i fałszywie dodatnich.

[21] Czułość testu diagnostycznego jest stosunkiem wyników prawdziwie dodatnich do sumy prawdziwie dodatnich i fałszywie ujemnych.

[22] Interpretacja swoistości i czułości testu diagnostycznego może nie być oczywista. Dla przykładu: jeśli test diagnostyczny ma czułość i swoistość równą 99% (a więc subiektywnie sprawiającą wrażenie wysokiej), przy badaniu 1000 osób, w 10 przypadkach test da wynik fałszywie pozytywny. Jeśli częstość występowania badanej cechy w populacji jest nierównomierna (np. pół procenta osób będących nosicielami choroby), to liczba wyników fałszywie pozytywnych lub fałszywie negatywnych może być na tyle duża, że nawet po pozytywnym (negatywnym) wyniku testu nadal bardziej prawdopodobne jest, że badany zidentyfikowanego wariantu cechy nie posiada (posiada) – prawdopodobieństwo całkowite może być mniejsze niż 50%.

[23] Zob. J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 372 i nast.

[24] Ibid.

[25] Zob. ibid., s. 560 i nast.

Dla badań DNA przyjmuje się następujące określenia ilorazu wiarygodności[26]:

- ✓ 1–10 – dowód słaby;
- ✓ 10–100 – dowód średni;
- ✓ 100–1000 – dowód mocny;
- ✓ powyżej 1000 – dowód bardzo mocny.

Oczywiście zarówno powyższe określenia, jak i progowe wartości liczbowe ilorazu wiarygodności, mają charakter arbitralny.

Podobnie arbitralnie ustala się dla potrzeb postępowań odszkodowawczych procent uszczerbku na zdrowiu, przypisany do różnych uszkodzeń ciała (np. utrata kończyny, utrata słuchu itd.), oczywistym jest, że nie można tu mówić o procentach *sensu stricto* (setnych częściach pojęcia „zdrowie"). Biorąc pod uwagę, że znajomość aktualnie przyjętej metodyki postępowania nie musi być powszechna (zarówno wśród stron postępowania, jak i wśród prawników), wydaje się być wskazanym – co najmniej z powodów dydaktycznych – dokładne informowanie w opinii o przyczynach takiej, a nie innej kategoryczności wniosków.

Z omawianą kwestią związana jest również możliwość zaniżenia kategoryczności wniosków przez osobę formułującą wnioski z badania. Niechęć do formułowania wniosków kategorycznych jest rozpowszechniona wśród przedstawicieli części dyscyplin naukowych. Za należące do dobrego stylu uznaje się sformułowania osłabiające kategoryczność wypowiedzi („jak się wydaje", „może być w niektórych przypadkach" itd.). Taka ostrożność jest oczywiście wskazana tam, gdzie przeprowadzone badania nie dają wyników jednoznacznych, wyniki badań z próby nie dają się uogólnić na populację, tam, gdzie zaobserwowane prawidłowości mają charakter wyłącznie statystyczny[27] itp.; natomiast jest niepotrzebna wszędzie tam, gdzie mowa o rzeczywistym i powtarzalnym, niebudzącym wątpli-

[26] Zob. E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka*…, op. cit., s. 533.

[27] A więc w szczególności bardzo często w naukach społecznych.

wości wyniku testu czy pomiaru. Negowanie możliwości poznania i sformułowania zdań prawdziwych można prowadzić tylko wychodząc z założeń skrajnego relatywizmu teoriopoznawczego[28].

Zdecydowanie należy też rozróżnić subiektywną (podmiotową) wiedzę o prawdzie, a samą prawdą[29]. W opiniowaniu sądowo-informatycznym stosunkowo często można w konkluzji umieszczać zdania pewne, np. „na

[28] Dobrym streszczeniem takiej postawy są sformułowania przytoczone przez L.F. Korzeniowskiego: „(…) prawda ma charakter względny i się zmienia. Prawda zawsze zależy od dowodów, metod i teorii znanych nauce" (L.F. Korzeniowski: *Podstawy*…, op. cit., s. 35).

[29] Tak pisze o tym J. Bocheński: „W rzeczywistości żadna prawda nie jest względna (…). Mówimy bowiem, że dane zdanie jest prawdziwe dokładnie wtedy, kiedy to, co ono znaczy, jest tak, jak ono znaczy. Np. zdanie »Grzmi teraz w Krakowie« posiada prawdę, jest prawdziwe, dokładnie o tyle, o ile w Krakowie rzeczywiście teraz grzmi. Jest prawdziwe względnie fałszywe całkiem niezależnie od tego, co ja albo ktokolwiek inny o owym grzmocie w Krakowie wie i sądzi.(…) jest wynikiem pomieszania dwóch całkiem różnych rzeczy, z jednej strony prawdy, z drugiej naszej wiedzy o tej prawdzie. Jest bowiem tak, że ludzka wiedza o prawdziwości zdań jest zawsze ludzka, to jest zależna od ludzkich podmiotów, jest więc – w tym słowa znaczeniu – zawsze względna. Natomiast sama prawda zdania nie ma z tą wiedzą nic wspólnego: zdanie jest prawdziwe albo fałszywe całkiem niezależnie od tego, czy ktoś tę prawdziwość względnie fałszywość zna, czy nie zna.
W naszym przykładzie, zakładając, że w tej chwili rzeczywiście grzmi w Krakowie, może doskonale się zdarzyć, że jeden człowiek, np. Jan, wie, że tak jest, a inny, np. Karol, nie wie i sądzi nawet, że nie grzmi teraz w Krakowie. Wówczas Jan wie, że odnośne zdanie – »Grzmi teraz w Krakowie« – jest prawdziwe, a Karol tego nie wie. Ich wiedza jest więc, jak powiedziano, zależna od tego, czyją jest wiedzą: inaczej mówiąc, jest względna. Ale prawdziwość, czy fałszywość tego zdania nie jest od tego zależna. Nawet gdyby nikt nie wiedział, że grzmi teraz w Krakowie, to gdyby tak rzeczywiście było, nasze zdanie byłoby bezwzględnie prawdziwe, niezależnie od tego, co Jan i Karol o nim wiedzą. Nawet takie zdanie jak »Liczba gwiazd w drodze mlecznej jest podzielna przez 17«, o których nikt nie wie, czy są prawdziwe, są prawdziwe albo fałszywe (…). Do tej samej »względności« dadzą się sprowadzić inne rzekome pojęcia prawdy, np. pojęcie pragmatyczne, dialektyczne i tym podobne. Wszystkie te zabobony powołują się na pewne trudności techniczne, w zasadzie jednak wynikają ze sceptycznej postawy człowieka, który wątpi w możliwość poznania czegokolwiek. Owe trudności techniczne są pozorne. Na przykład mówi się, że powiedzenie »Grzmi teraz w Krakowie« może być prawdziwe dziś, ale będzie fałszywe jutro, kiedy w Krakowie nie będzie grzmiało. Mówi się także, że np. zdanie »pada« jest prawdziwe we Fryburgu, ale fałszywe w Tarnowie, kiedy pada w pierwszym mieście, a słońce świeci w drugim. Są to jednak nieporozumienia: wystarczy wspomniane zdania uściślić, powiedzieć np., że przez »teraz« rozumiemy 1 lipca 1987 r., godzinę 10 i 15 minut wieczorem, aby usunąć ową rzekomą względność. Prawda jest

dysku znaleziono plik zawierający zapisy, o których mowa w pytaniu", „komputer jest uszkodzony" itd., niepozostawiające wątpliwości co do bezwzględnego charakteru stwierdzonych faktów[30]. Informatycy mają zresztą raczej skłonność do nieuzasadnionego zawyżania niż do zaniżania kategoryczności swoich wypowiedzi. Jak pisze Kazimierz Jaegermann[31]: „Język konkluzji opiniodawczej nie może stwarzać żadnych językowych wątpliwości co do tego, czy biegły *wie*, czy też, że biegły jest tylko *pewien*".

1.3 „Dyscypliny pomostowe" a klasyfikacje dyscyplin naukowych

Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (dalej ROWDN), które wprowadziło w Polsce trójstopniową klasyfikację dyscyplin naukowych, pomija milczeniem problematykę dyscyplin pomostowych oraz dyscyplin związanych, z wymiarem sprawiedliwości. Nie ma w nim ani – najstarszej spośród nauk sądowych – medycyny sądowej, ani psychiatrii sądowej, ani kryminalistyki, ani kryminologii. Również rozporządzenie Ministra Pracy i Polityki Społecznej z 27 kwietnia 2010 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz jej stosowania (dalej RKZIS) wśród zawodów „śledczych" wyróżnia jedynie zawód „Dyrektora aresztu śledczego/ zakładu karnego" (kod 134901), zaś wśród zawodów sądowych dwie pozycje „Lekarz – medycyna

bezwzględna albo jej nie ma (…)" (J. Bocheński: *Sto zabobonów. Krótki filozoficzny słownik zabobonów*, PHILED, Kraków 1994).

[30] Oczywiście nie można pominąć milczeniem omylności biegłych, czy też ich podatności na wpływy kontekstowe (por. np. J. Wójcikiewicz: *Temida…*, op. cit., s. 26 i nast.; J. Kunz: *Błąd…*, op. cit.; Z. Marek: *Błąd medyczny*, Wydawnictwo Medyczne, Kraków 2007, s. 101 i nast.), niemniej aprioryczne zaniżanie kategoryczności wniosków w oparciu o antycypację możliwości popełnienia błędu przez osobę formułującą wniosek ma charakter nie bardzo uzasadnionej autocenzury. Jeśli już biegły uznaje, że powinien podkreślić subiektywny (podmiotowy) charakter prowadzonego badania to należy uczynić to raczej za pomocą sformułowań „zdaniem biegłego", „biegły doszedł do wniosku", czy „z badań przeprowadzonych przez biegłego wynika" niż – właściwych raczej mowie potocznej – wyrażeń „o ile się nie mylę", „o ile dobrze zrozumiałem" itd.

[31] K. Jaegermann: *Opiniowanie sądowo-lekarskie. (Eseje o teorii)*, Wydawnictwo prawnicze, Warszawa 1991, s. 132–133.

sądowa" (kod 221237) oraz „Diagnosta laboratoryjny – laboratoryjna diagnostyka sądowa" (kod 227204).

Jak się wydaje, pisząc o informatyce sądowej (jak i o innych dyscyplinach sądowych), należy zatem spróbować przede wszystkim umiejscowić je wśród rzeczywiście istniejących (niekoniecznie urzędowo zatwierdzonych[32]) nauk i dyscyplin naukowych. Kryminalistyka w sposób oczywisty wiąże się z naukami prawnymi, stąd też dużą część naukowców, zajmujących się jej zagadnieniami, stanowią prawnicy; również studia (najczęściej podyplomowe) z zakresu kryminalistyki organizowane są w dużej mierze na wydziałach prawa uniwersytetów. Z drugiej strony opiniowanie w konkretnych sprawach wymaga znajomości poszczególnych nauk (technicznych, ekonomicznych, medycznych itd.) bądź technik kryminalistycznych, stąd też zagadnienia związane z diagnostyką stanów istniejących i ustalaniem ich przyczyn z natury rzeczy mieszczą się w obrębie poszczególnych dyscyplin szczegółowych (informatyki, chemii, weterynarii, medycyny itd.). Z trzeciej wreszcie strony zagadnienia związane z zabezpieczaniem materiału dowodowego i jego analizą związane są z praktyką pracy policji i służb specjalnych, stąd też zagadnienia tego rodzaju są przedmiotem prac specjalistów ze szkół policyjnych[33].

[32] Rozporządzenie ROWDN wprowadziło zresztą kilka rozwiązań co najmniej dyskusyjnych – np. da się w nim znaleźć dyscyplinę „biocybernetyka i inżynieria biomedyczna", nie ma natomiast cybernetyki, jest dyscyplina „bibliologia i informatologia", przy czym słowa „informatologia" nie ma w żadnym słowniku języka polskiego – jest to neologizm zapożyczony, jak się zdaje, z języka chorwackiego (zob. np.: strona główna czasopisma „Informatologia", http://hrcak.srce.hr/index.php?show=casopis&id_casopis=129&lang=en) itd. Na szczęście rozporządzenie nie ogranicza ani istnienia jednostek naukowych, które mogą zajmować się niewymienionymi w nim naukami i dyscyplinami (np. Wydział Cybernetyki Wojskowej Akademii Technicznej, http://www.wcy.wat.edu.pl), ani kierunków i rodzajów studiów (np. Studia Podyplomowe Kryminalistyki na Uniwersytecie Wrocławskim, http://podyplomowe.prawo.uni.wroc.pl/userfiles/file/SPK%20prof_%20dr%20hab%2013_03_2014.pdf).

[33] Zob. H.G. Jaschke: *Policyjna nauka – podejście europejskie*, CEPOL 2008, https://www.cepol.europa.eu/fileadmin/website/Research_Science/PGEAPS/PGEAPS_summary_polish.pdf; *Perspectives of police science in Europe, CEPOL 2007*, https://www.cepol.europa.eu/fileadmin/website/Research_Science/PGEAPS_Final_Report.pd.

Rozporządzenie ROWDN potwierdziło wprawdzie istnienie osobnej dyscypliny „Nauki o bezpieczeństwie", wprowadzonej uchwałą Centralnej Komisji do Spraw Stopni i Tytułów z 28 stycznia 2011 r. zmieniającą uchwałę w sprawie określenia dziedzin nauki i dziedzin sztuki oraz dyscyplin naukowych i artystycznych (dalej UCKSST), która to dyscyplina zajmuje się kwestiami związanymi m.in. z funkcjonowaniem niemilitarnych systemów bezpieczeństwa, natomiast umiejscowienie tej dyscypliny w obszarze nauk społecznych budzi pytanie o możliwość rozpatrywania w ich ramach zagadnień technicznych (inżynieria bezpieczeństwa)[34].

Nie można z faktu administracyjnego przyporządkowania dyscypliny naukowej do obszaru wyciągać zbyt daleko idących wniosków: nauki o obronności również znajdują się w obszarze nauk społecznych, a nikt poważnie nie może negować ani praktycznego znaczenia, ani wkładu, jaki do nauki wnoszą osiągnięcia techniki wojskowej[35].

Oczywiście takie formalno-administracyjne rozproszenie nie tworzy dobrych warunków do rozwoju nauki ani techniki, stąd też w dziedzinie informatyki sądowej (śledczej) powstaje stosunkowo mało oryginalnych polskich prac naukowych, jak również rozwiązań technicznych[36].

---

[34] W umieszczeniu nauk o bezpieczeństwie w obszarze nauk społecznych można dopatrywać się również aspektów pozytywnych (z punktu widzenia podjętej w pracy tematyki). Jak pisze Leszek F. Korzeniowski: „Warto w tym miejscu przypomnieć iż prawo, jako dyscyplina naukowa, zostało usytuowane w dziedzinie nauk prawnych w tym samym co nauki o bezpieczeństwie obszarze nauk społecznych. To wyraźna sugestia skierowana do przedstawicieli nauk o bezpieczeństwie oraz do przedstawicieli nauk prawnych o poszukiwanie wspólnych zakresów podmiotowych, przedmiotowych i metodologicznych w nowo wyodrębnionym, wspólnym dla obydwu dziedzin obszarze nauk społecznych" (L.F. Korzeniowski: *Nauki o bezpieczeństwie – wprowadzenie do problematyki* [w:] P. Cybula: *Prawne aspekty bezpieczeństwa w górach: turystyka, rekreacja, sport*, pod red. P. Cybuli, COTG PTTK, Kraków 2013, s. 257–272).

[35] Zob. np.: Ľ. Čech: *Bezpečnostné aspekty vzdelávania profesionálov ozbrojených síl SR – pohľad učiteľa spoločenských vied* [w:] *Bezpečnosť a bezpečnostná veda*, Liptovský Mikuláš: Akadémia ozbrojených síl generála M. R. Štefánika, 2009, s. 219-224.

[36] Wyjątkiem zdają się tu być – znajdujące się jednak poza obszarem rozważań zawartych w tej monografii – narzędzia do komputerowego wspomagania analizy kryminalnej, które są przedmiotem badań na kilku uczelniach w Polsce (zob. np.: P. Chlebowicz*: Perspektywy wykorzystania analizy kryminalnej w praktyce prokuratorskiej*, „Prokuratura i Prawo" Nr 7–8/2013, s. 263–277; K. Cetnarowicz, R. Cięciwa, E. Nawarecki, G. Rojek: *Unfavorable Behavior Detection in Real World Systems Using the Multiagent System,* Intelligent Information Systems, 2005,

Rozwiązanie (funkcjonujące w części państw europejskich, np. na Słowacji[37] czy w Czechach), w którym nauki policyjne są wyodrębnione jako osobna dyscyplina naukowa, wydaje się być z pragmatycznego punktu widzenia o wiele korzystniejsze.

s. 416–420; M. Kobylas: *Analiza kryminalna w Polsce. Ewolucja w kierunku GIS*, http://www.konferencja.esri.pl/sites/default/files/M.Kobylas_WSP%20w%20Szczytnie.pdf).

[37] Por. np.: V. Porada, K. Holcr, et al.: *Policejní vědy*, Vyd. Aleš Čeněk, Plzeň 2011; J. Meteňko, K. Líška: *Riadenie operatívnych činností*, Akadémia Policajného Zboru, Bratislava 2003; S. Uhrín, P. Selinger: *Bezpečnostné služby*, Žilinská univerzita, Žilina 2003.

2 Opiniodawcza rola informatyki

Mówiąc o dyscyplinach sądowych należy przede wszystkim dokonać rozróżnienia pomiędzy nimi a technikami kryminalistycznymi. Najstarszą z dyscyplin sądowych jest oczywiście medycyna sądowa[38]. Współcześnie wśród biegłych sądowych, obok medyków sądowych[39], szczególną rolę zajmują psychiatrzy oraz ekonomiści, zwłaszcza biegli sądowi z zakresu rachunkowości[40]. We współczesnej literaturze fachowej używa się nazw dyscyplin, takich jak np. – obok wspomnianej już medycyny sądowej – psychiatria sądowa czy psychologia sądowa. Dyscypliny te zwane są czasem „naukami pomostowymi" z uwagi na rolę łącznika, jaką pełnią pomiędzy „czystą" dyscypliną a naukami prawnymi. Kwestią czasu jest, jak się zdaje, powstanie kolejnych nauk sądowych również w obrębie innych nauk, w szczególności technicznych i stosowanych[41].

---

[38] Pierwsza na ziemiach polskich i trzecia w Europie Katedra Medycyny Sądowej powołana została w 1804 r. na Uniwersytecie Jagiellońskim w Krakowie (zob. Z. Marek: *Wybrane problemy opiniowania sądowo-lekarskiego*, Zakamycze, Kraków 2004, s. 9).

[39] Mianem medyków sądowych określa się w literaturze lekarzy opiniujących w sprawach sądowych, ze specjalnością medycyna sądowa, w odróżnieniu od „klinicytów", tj. lekarzy innych specjalności (zajmujących się głównie leczeniem, a nie opiniowaniem). Odrębnym pojęciem (prawnym) jest pojęcie lekarzy sądowych, tj. lekarzy wystawiających zaświadczenia potwierdzające zdolność albo niezdolność do stawienia się na wezwanie lub zawiadomienie organu uprawnionego uczestników postępowania z powodu choroby. Zob. ustawa z 15 czerwca 2007 r. o lekarzu sądowym (dalej ULS).

[40] Należy rozróżnić pojęcia: biegłych sądowych z zakresu ekonomii i jej poszczególnych dziedzin (biegłych sądowych z zakresu rachunkowości, biegłych sądowych z zakresu szacunku nieruchomości, biegłych sądowych z zakresu marketingu itd.), biegłych rewidentów. Zob. ustawa o biegłych rewidentach i ich samorządzie (dalej UBRIS) i biegłych skarbowych oraz ustawa z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (dalej UPEA).

[41] Na przykład pierwsza w Polsce pracownia chemii sądowej powstała kilka lat temu na Wydziale Chemii Uniwersytetu Jagiellońskiego, http://www2.chemia.uj.edu.pl/pracownia.php?id=10055.

2.1 Informatyka sądowa

Oprócz nauk sądowych wyróżnia się szereg dyscyplin (technik) kryminalistycznych. Kryminalistyka jest to nauka o taktycznych zasadach i sposobach oraz o technicznych metodach i środkach rozpoznawania, a także wykrywania prawnie określonych, ujemnych zjawisk społecznych, a w szczególności przestępstw i ich sprawców oraz udowadniania istnienia lub braku związku między osobami a zdarzeniami, a także zapobiegania przestępstwom i innym niekorzystnym, lecz prawnie relewantnym zjawiskom[42]. Istnieją różne podziały dyscyplin kryminalistycznych:

- ✓ na taktykę kryminalistyczną, techniki kryminalistyczne, strategię kryminalistyczną oraz metodykę kryminalistyczną[43];
- ✓ na taktykę kryminalistyczną, technikę kryminalistyczną i profilaktykę kryminalistyczną[44];

czy wreszcie

- ✓ na taktykę, technikę i strategię kryminalistyczną[45].

Poszczególne techniki kryminalistyczne to np.: mechanoskopia (badanie śladów pozostawionych przez narzędzia), daktyloskopia (badania porównawcze linii papilarnych), fonoskopia (badanie zapisów dźwięków), cheiloskopia (analizowanie śladów czerwieni wargowej), traseologia (badanie śladów przemieszczania się odciśniętych w podłożu), osmologia (badanie śladów zapachowych ludzi z wykorzystaniem specjalnie wyszkolonych w tym zakresie psów) itd.

W odniesieniu do informatyki należy, jak się zdaje, postulować raczej wyodrębnienie informatyki sądowej jako osobnej dyscypliny naukowej[46],

Na licznych polskich uniwersytetach istnieją specjalności (bądź studia podyplomowe) o nazwie „biologia sądowa" (np. Uniwersytet Łódzki, http://www.uni.lodz.pl/studia/studium,tematyka,489; Uniwersytet Adama Mickiewicza w Poznaniu, http://studenci.amu.edu.pl/studia/podyplomowe/wydzia-biologii/studia-podyplomowe-biologii-sdowej; Uniwersytet Przyrodniczy w Lublinie, http://wip.up.lublin.pl/medialne/?page=4&rid=2396).

[42] Zob. T. Hanausek: *Kryminalistyka*…, op. cit., s. 23 i nast.

[43] Ibid., s. 18.

[44] Zob. S. Kozdrowski: *Kryminalistyka*…, op. cit., s. 19.

[45] Zob. E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka*…, op. cit., s. 21–22.

[46] Jedyną jednostką naukową, która posługuje się pojęciem „informatyki sądowej" jest pracownia informatyki sądowej krakowskiego Instytutu Ekspertyz Sądowych im. prof. dra Jana Sehna, http://ies.krakow.pl/blog/struktura/pracownia-informatyki-sadowej. Pojęcie „infor-

a nie tylko techniki kryminalistycznej. Dzieje się tak przynajmniej z trzech powodów.

Przede wszystkim, z uwagi na bardzo szybkie, nieporównywalne z innymi dyscyplinami, tempo rozwoju technik informacyjnych i telekomunikacyjnych, zmianom ulega przedmiot badań biegłego informatyka: oprócz komputerów stają się nim inne urządzenia, jak odbiorniki GPS, telefony komórkowe, dyktafony cyfrowe itp. Zmienia się też sposób przetwarzania danych: od klasycznej sytuacji, w której dane zgromadzone są na pamięci masowej wbudowanej w urządzenie, poprzez popularyzację pamięci przenośnych, aż do modelu przetwarzania danych „w chmurze" (ang. *cloud*), a także rozmiar danych (a co za tym idzie – czas konieczny do ich analizy), z jakimi do czynienia mają osoby prowadzące badanie. Aspekty te wymuszają stosowanie nie tylko zupełnie innych technik badawczych, ale innych podejść (od podejścia klasycznego, z pełną statyczną analizą danych prowadzoną na kopii binarnej nośnika, do zyskujących obecnie popularność – analizy typu *live* i *triage*[47]). Dość dziwnie brzmiałoby mówienie o „kryminalistyce komputerowej" w sytuacji, w której przedmiotem badań jest nie komputer, a np. cyfrowy aparat fotograficzny.

matyki sądowej" zostało też użyte w książce: M. Szmit, A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec: *Elementy*…, op. cit. Równolegle, szczególnie wśród firm komercyjnych, funkcjonuje pojęcie „informatyki śledczej" (zob. np.: http://www.mediarecovery.pl; http://www.dabi.pl; T. Dyrda: *Informatyka śledcza*, V Międzynarodowy kongres audytu, kontroli wewnętrznej oraz procedur zwalczania oszustw i korupcji, Kraków 2006, http://webapp01.ey.com.pl/EYP/WEB/eycom_download.nsf/resources/Informatyka_sledcza_TD_pl.pdf/$FILE/Informatyka_sledcza_TD_pl.pdf, http://www.siis.org.pl). Używane jest również określenie „kryminalistyka komputerowa" (albo „informatyka kryminalistyczna" – zob. np.: E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka*…, op. cit., s. 559), a nawet – będące nowotworem językowym – pojęcie „forensyka komputerowa" (ang. *computer forensics*) – zob np.: L. Kordylewski: *Forensyka, Forensic Science Center*, http://www.kordynet.com/forensyka.html. Według materiałów firmy Novell (http://www.novell.com/poland/resourcecenter/novell_audit_charakterystyka_techniczna.pdf), „Termin *computer forensics* został po raz pierwszy użyty w 1991 r. podczas pierwszej sesji szkoleniowej prowadzonej w Portland w stanie Oregon przez International Association of Computer Specialists (IACS)".

[47] Zob. np.: M.K. Rogers, J. Goldman, R. Mislan, T. Wedge: *Computer Forensics Field Triage Process Model*, Conference on Digital Forensics, Security and Law 2006, http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf; J.J. Barbara: *Triage A Computer*, "Forensic Magazine", http://www.forensicmag.com/articles/2010/06/triage-computer#.Ur34p42x9i4.

Po wtóre, rola biegłego informatyka w sądzie nie ogranicza się do spraw *stricte* kryminalnych[48]. Rzecz jasna, również działalność techników kryminalistyki nie jest ograniczona do spraw karnych[49], niemniej biegli informatycy stosunkowo często wydają opinie, które nie dotyczą analizy śladów dowodowych, ale sposobu działania narzędzi informatycznych czy metod stosowanych w komputerowym przetwarzaniu danych. Intuicyjnie zrozumiałe jest, że np. biegły z zakresu wspomnianej wcześniej cheiloskopii nie ma raczej zbyt wielu okazji do opiniowania na temat pracy specjalistów z tej dziedziny (wyjąwszy ewentualne metaopinie[50]), podczas gdy biegły informatyk stosunkowo często wypowiada się np. w sprawach związanych z ustaleniem praw autorskich do programów komputerowych, w sprawach dotyczących domniemanego złego wypełniania obowiązków przez osoby bądź firmy outsourcingowe, którym powierzono opiekę nad systemem informatycznym, czy w sprawach dotyczących procesu informatyzacji organizacji gospodarczych. Nie ma w takich opiniach – charakterystycznych dla technik kryminalistycznych – zabezpieczania i analizy śladów dowodowych jest natomiast konieczność głębokiej znajomości poszczególnych dyscyplin informatycznych (np. inżynierii oprogramowania czy informatyki ekonomicznej), zarówno od strony praktycznej, jak i od strony obowiązujących standardów czy powszechnie przyjętych dobrych praktyk.

Trzecim argumentem, który należałoby podnieść, jest niewątpliwy wpływ uregulowań prawnych na rozwój samej informatyki. Można tu wspomnieć choćby o wpływie przyjętego modelu ochrony prawnoautorskiej[51] na rozwój oprogramowania (w tym ruchu wolnego oprogramowania); o wpływie praktyki stosowania prawa (w tym dopuszczalności i roz-

[48] Słowo „kryminalny" pochodzi z łacińskiego *crimen* (przestępstwo), stąd też popularny związek frazeologiczny „przestępstwa kryminalne" jest poniekąd pleonazmem.

[49] Metody badawcze opracowane dla potrzeb kryminalistycznych stosowane są również w procesach cywilnych, a nawet w dziedzinach pozaprocesowych, np. archeologii (zob. np.: S. Kozdrowski: *Kryminalistyka*…, op. cit., s. 18).

[50] To jest opinie o opiniach (zob. np.: G. Kopczyński, *Konfrontacja*…, op. cit., s. 187 i nast.; J. Wójcikiewicz: *Temida*…, op. cit., s. 25 i nast.; J. Wójcikiewicz: *Metaopinie – wyraz siły czy słabości wymiaru sprawiedliwości. Biegły w sądzie*, materiały konferencyjne, Wydawnictwo Instytutu Ekspertyz Sądowych, Kraków 2006 s. 103–106. Zob. też rozdział 3.7.

[51] A także trwającej ciągle, choć w mniejszym natężeniu niż kilka lat temu, dyskusji o możliwości stosowania modelu ochrony patentowej do programów komputerowych.

powszechnienia metod inwigilacji) na rozwój kryptografii; o związkach pomiędzy uregulowaniami prawnymi (i praktyką orzeczniczą) w zakresie odpowiedzialności cywilnej i karnej za uzyskiwanie bądź użytkowanie oprogramowania wbrew wymogom licencyjnym a tempem rozwoju usług doradztwa informatycznego, w tym tzw. audytu legalności oprogramowania; o całej gamie zagadnień dotyczących transgraniczności Internetu, a więc możliwości umieszczenia konkretnych usług czy treści pod rządami różnych systemów prawnych, dla osiągnięcia nie tylko zysków natury ekonomicznej, ale wręcz możliwości popełniania czynów niepenalizowanych w prawie krajowym[52].

Stąd też konsekwentnie w książce używane jest pojęcie informatyki sądowej, choć poruszane są zagadnienia dotyczące również innych (niż sala sądowa) okoliczności opiniowania przez osoby zajmujące się informatyką.

2.2 Informatyk jako rzeczoznawca, doradca i audytor[53]

W praktyce biznesowej i życiowej konieczne jest niejednokrotnie korzystanie z wiedzy niezależnego eksperta. Z metodologicznego punktu widzenia należałoby rozróżnić trzy role, jakie niezależny fachowiec może pełnić w stosunku do swojego klienta:

- ✓ przede wszystkim może on występować jako rzeczoznawca, który ma za zadanie wyjaśnić wątpliwości odnośnie do stanu faktycznego, jego przyczyn i implikacji oraz służyć swojemu klientowi fachową wiedzą i doświadczeniem z zakresu reprezentowanej specjalności. Rolą rzeczoznawcy jest więc w głównej mierze wypowiadanie się w sprawie stanów rzeczowych (co można wywieść z ety-

[52] Przykładem w odniesieniu do polskiego systemu prawnego może być umorzenie sprawy witryny RedWatch (administratorem strony jest firma amerykańska, zaś Stany Zjednoczone odmawiają pomocy prawnej w tego typu sprawach, powołując się na I poprawkę do konstytucji USA). Można znaleźć również inne przykłady, w szczególności związane z prawem autorskim czy zakazem „hazardu internetowego". Oczywiście rozwijanie takich usług wymaga wykorzystania infrastruktury informatycznej, a więc – niezależnie od prawnej czy moralnej oceny samych czynów – ma wpływ przynajmniej na wykorzystanie narzędzi informatyki.

[53] Wykorzystano fragmenty artykułu: M. Szmit: *Informatik jako expert v podmínkách polského legislativního system. Metodologické úvahy, Internet, Competitiveness and Organizational Security*, Tomas Bata University Zlín 2010.

mologii tego wyrazu). Rzeczoznawca opiera się w swoim opiniowaniu na powszechnie przyjętych standardach wnioskowania oraz na użyciu narzędzi badawczych. Zadaniem rzeczoznawcy jest:

- diagnostyka identyfikacyjna, odpowiadająca na pytanie „jaki jest obecny stan rzeczy",
- diagnostyka kauzalna (genetyczna), odpowiadająca na pytanie „jakie są jego przyczyny"[54]

oraz

- w ograniczonym zakresie diagnostyka prognostyczna[55], odpowiadająca na pytanie „w jaki sposób ten stan powinien się rozwinąć w przyszłości"[56].

[54] W niektórych naukach używa się pojęcia „retrognoza" (zob. np.: J. Paradysz, M. Szymkowiak: *Źródła danych ludnościowych. Metodologia Badań Demograficznych*, Zeszyt nr 15 Sekcji Analiz Demograficznych PAN, s. 7–26, http://www.ae.krakow.pl/~demograf/Publikacje/SAD15.pdf).

[55] Pojęcie „diagnoza prognostyczna" może brzmieć nieco dziwnie, tradycyjnie bowiem diagnozę (z greckiego διάγνωση *od* διά – rozdzielić i γνώση – wiedza, poznanie) przeciwstawia się prognozie (z greckiego πρόγνωση od πρό– przed i γνώση – wiedza, poznanie). Zgodnie z tym „diagnozowanie to wnioskowanie polegające na ocenie zjawiska w przeszłości (wnioskowanie *ex post*, wnioskowanie w obrębie próby), a prognozowanie to wnioskowanie polegające na przewidywaniu wartości określonych zmiennych w przyszłości (wnioskowanie *ex ante* – wnioskowanie poza próbę" (A. Zeliaś, B. Pawełek, S. Wanat: *Prognozowanie ekonomiczne*, Wydawnictwo Naukowe PWN, Warszawa 2003, s. 13), niemniej z bardziej ogólnego punktu widzenia przeprowadzenie analizy jakiegoś systemu bądź zjawiska może prowadzi do uzyskania wiedzy o jego zachowaniach, która pozwala zarówno na wnioskowanie o jego stanie obecnym, jak i – z pewnym prawdopodobieństwem – o jego stanach przeszłych i przyszłych (o ile oczywiście poznane reguły rządzące obecnie zachowaniem systemu można ekstrapolować na jego zachowania wcześniejsze i późniejsze). Stąd też w części dyscyplin – w szczególności humanistycznych – mówi się właśnie o diagnostyce prognostycznej (por. np. B. Batóg, K. Wawrzyniak: *Diagnozowanie a prognozowanie ekonometryczne – podobieństwa, różnice, zależności*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" Nr 394, „Prace Katedry Ekonometrii i Statystyki" Nr 15/2004, Szczecin 2004, s. 21–33; S. Ziemski: *Problemy dobrej diagnozy*, PWN, Warszawa 1973). Nie wnikając w subtelności znaczeniowe, można założyć, że proste rozważania dotyczące przyszłego zachowania systemu, powstałe przez ekstrapolację poznanych reguł nim rządzących poza próbę, da się zaliczyć do zadań rzeczoznawcy, natomiast budowanie złożonych prognoz, zawierających obszerne założenia co do przyszłych zdarzeń, jest raczej rolą doradcy niż eksperta.

[56] Oczywiście, o ile o stanie obecnym można wypowiadać się ze stosunkowo największą pewnością, o tyle ustalanie przyczyn i prognozowanie dalszego przebiegu zjawiska obarczone jest zazwyczaj większą niepewnością. Stąd też, o ile do oceny diagnozy identyfikacyjnej można stosować kryterium prawdziwości (zgodności ze stanem rzeczywistym), o tyle

Wykonywanie tego rodzaju ekspertyz jest w Polsce stosunkowo rzadkie. Najczęściej po radę do eksperta zgłaszają się organizacje bądź to będące już w sporze sądowym, bądź to przygotowujące się do takiego, ewentualnie próbujące łagodzić skutki jakiegoś zdarzenia związanego z wystąpieniem problemów natury technicznej czy ekonomicznej. Zadania rzeczoznawcy są – w pewnym zakresie – podobne do roli biegłego, stąd też ekspertyza będąca efektem pracy takiej osoby, jeśli dojdzie do jej wykorzystania w postępowaniu sądowym, nazywa się czasem potocznie „opinią pozasądową" (lub „opinią prywatną"), zaś sam ekspert – „biegłym prywatnym"[57], przy czym powstałe w sen sposób opinie prywatne z prawnego punktu widzenia mają stosunkowo małe znaczenie: jeśli dojdzie do postępowania sądowego, nie są traktowane jako dowody, ale jedynie jako dokumenty prywatne[58] (wypowiedzi strony w sprawie)[59]; niemniej nie można ich pominąć[60];

przy ocenie prognoz czy retrognoz (diagnoz kauzalnych, genetycznych), bardzo istotna jest formalna ocena poprawności sposobu wnioskowania.

[57] Dla odróżnienia od biegłego sądowego, którego to określenia wolno używać tylko po powołaniu przez sąd bądź organ prowadzący postępowanie przygotowawcze w sprawie karnej.

[58] Por. wyrok Sądu Najwyższego z 8 czerwca 2001 r. (I PKN 468/00): „Jeżeli (…) strona składa pozasądową ekspertyzę z wyraźną intencją potraktowania jej jako dowodu w sprawie, wówczas istnieją podstawy do przypisania jej rangi dowodu z dokumentu prywatnego (art. 245 KPC).(…) Pozasądowa opinia rzeczoznawcy traktowana jako dokument prywatny stanowi dowód tego, że osoba, która ten dokument podpisała, prezentuje pogląd przedstawiony w dokumencie. Nie ma istotnych argumentów przemawiających za pominięciem takiego dowodu przez sąd przy ocenie materiału zebranego w sprawie".

[59] Por. wyrok Sądu Najwyższego z 10 grudnia 1998 r. (I CKN 922/97): „Podkreślić trzeba, że pisemna opinia złożona do akt innej sprawy nie ma charakteru dowodu z opinii biegłego, gdyż sąd nie wydał postanowienia w przedmiocie dopuszczenia tego dowodu, nie wyznaczył biegłego i nie zakreślił mu przedmiotu i granic, w jakich ma się on wypowiedzieć". Sytuacja taka jest m.in. uzasadniona tym, że ekspert, przygotowujący tego rodzaju opinię, może nie dysponować całością materiału badawczego. Zdarzają się sytuacje, w której dwie opinie prywatne przygotowane przez wysokiej klasy ekspertów na zlecenie dwóch stron pozostających w sporze zawierają przeciwne wnioski, jako że opracowane były na podstawie różnych materiałów (dostarczonych przez strony). Praktyka stosowania opinii prywatnych jest w Polsce stosunkowo rozpowszechniona w przypadku sporów dotyczących praw zamówień publicznych toczących się przed Krajową Izbą Odwoławczą.

- ✓ po wtóre, ekspert może pełnić funkcję doradcy rekomendującego klientowi wybór strategii i taktyki działania, a nawet sugerującego, jaki powinien być pożądany stan docelowy. Z oczywistych względów (zazwyczaj pomoc doradcy potrzebna jest tam, gdzie istnieją rozbieżności odnośnie do planowanych celów czy sposobów ich osiągnięcia), doradca może, a nawet powinien, pozwolić sobie na znacznie dalej idący subiektywizm wypowiedzi niż rzeczoznawca (rozumiany tak, jak powyżej). Rolą doradcy jest wsparcie klienta w procesie decyzyjnym nie tylko poprzez dostarczenie mu informacji na temat przeszłych (retrognozowanych), aktualnych czy przyszłych (prognozowanych) stanów rzeczowych, ale przez zasugerowanie pożądanych stanów docelowych i strategii ich osiągnięcia czy taktyki poszczególnych działań. Oczywiste jest, że ocena poprawności proponowanej strategii postępowania *ex post* może opierać się o osiągnięte efekty, natomiast *ex ante* – bardzo często jedyną metodą oceny jakości prognozy czy strategii pozostaje badanie zgodności proponowanego sposobu działania z praktykami działania (najlepszymi praktykami) obowiązującymi w danej dziedzinie. Jest sytuacją dość powszechną, przynajmniej w informatyce, że praktyki takie są nie do końca spójne ze sobą, zaś decyzje podejmowane są w warunkach niepełnej informacji[61]. W takich sytuacjach znaczny wpływ na sugerowane przez doradcę decyzje mogą mieć jego osobiste doświadczenia i upodobania. W interesie zarówno samego eksperta, jak i jego klienta leży wyraźne rozdzielenie roli rzeczoznawcy i doradcy. W przeciwnym razie osoba zamawiająca usługę doradztwa może odnieść wrażenie, że sugerowany przez doradcę sposób roz-

[60] Por. wyrok Sądu Najwyższego z 29.10.1990 r. (V KO 8/90): „nie można takiego dokumentu pominąć (...), gdyż zawiera on informacje o dowodzie, który nie jest pozbawiony znaczenia dla prawidłowego rozstrzygnięcia sprawy".

[61] Gdyby informacja była pełna, zaś reguły działania całkowicie znane i zalgorytmizowane, nie można by mówić w ogóle o sytuacji decyzyjnej. Ta bowiem występuje wtedy, gdy do wyboru istnieje więcej niż jedna droga postępowania. Problemem, z którym zresztą na co dzień spotykają się osoby zajmujące się informatyką (szczególnie informatyką ekonomiczną), jest raczej nadmiar niż niedobór rozmaitych metodyk, modeli i standardów rekomendujących – często na bardzo wysokim poziomie abstrakcji – sposoby postępowania przy wdrożeniu czy eksploatacji systemów informatycznych.

wiązania problemu jest jedynym możliwym i że narzucają go naukowe bądź techniczne reguły rządzące daną dyscypliną wiedzy, podczas gdy jest to tylko subiektywna, przynajmniej w jakiejś mierze, opinia autora ekspertyzy[62]. Postępowanie przeciwne (niestety dość częste zarówno w informatyce, jak i w innych dziedzinach) należy ocenić nagannie.

Problem oceny działalności doradczej pojawia się również w praktyce prac biegłych informatyków: informatyzacja jakiegoś obszaru działalności danej organizacji (firmy, urzędu) wiąże się bowiem zazwyczaj nie tylko z prostą automatyzacją wykonywanych prac biurowych, ale z daleko posuniętą ingerencją w kształt zachodzących w niej procesów informacyjno-decyzyjnych. Stąd też konsekwencje takiej (szczególnie nieudanej) informatyzacji odczuwalne są w działaniu całej organizacji, a nierzadko prowadzą nawet do niemożliwości dalszego jej działania[63]. Spory z tym związane kończą się często na sali sądowej, gdzie rolą biegłego informatyka jest pomoc sądowi w ocenie prawidłowości postępowania osób i firm zaangażowanych w proces informatyzacji. Prawidłowość owa powinna w takich wypadkach być rozstrzygana nie w oparciu o osiągnięte *ex post* efekty (zgodnie ze schematem: gdyby te efekty były satysfakcjonujące, to sprawa nie trafiłaby do sądu, więc – jeśli do niego trafiła – to podjęte działania nie były prawidłowe), ale w oparciu o zgodność z najlepszymi praktykami prowadzenia przedsięwzięć i to według wiedzy aktualnej w czasie prowadzenia projektu, a nie w czasie trwania procesu sądowego. Biorąc pod

[62] Postulat ten został zawarty w Kodeksie Zawodowym Informatyka Polskiego Towarzystwa Informatycznego, http://www.pti.org.pl/index.php/corporate/Kodeks-Zawodowy-Informatykow-PTI, w punktach 7 i 8:

„7. Informatycy prowadzący wolną działalność dydaktyczną prezentując konkretne rozwiązania zawsze starają się przedstawić możliwie szerokie spektrum rozwiązań o analogicznej funkcjonalności oraz przeznaczeniu, jeśli takie istnieją. Analogicznie starają się w tego rodzaju działalności oddzielać własne poglądy w konkretnej sprawie od innych istniejących poglądów.

8. Informatycy prowadzący działalność naukową lub badawczo-rozwojową zawsze wyraźnie oddzielają wiedzę pewną i już udowodnioną od przyjmowanych przez siebie założeń".

[63] Zob. np.: M. Szmit: *Informatyka w Zarządzaniu*, Centrum Doradztwa i Informacji Difin, Warszawa 2003.

uwagę tempo rozwoju informatyki, nieporównywalne z żadną dziedziną ludzkiej aktywności oraz – niestety pozostawiające dużo do życzenia – tempo postępowań sądowych w Polsce, trzeba dostosowywać wiedzę, w oparciu o którą wydawana jest opinia, do momentu zaistnienia zdarzeń, o których w niej mowa. Autorowi niejednokrotnie zdarzyło się opiniować na temat zdarzeń, które miały miejsce osiem czy dziewięć lat przed wydaniem opinii (a więc w sytuacji, gdy na rynku były dostępne zupełnie inne narzędzia informatyczne, obowiązywały inne normy i standardy techniczne, a poziom rozwoju wiedzy był nieporównanie niższy niż w chwili wydania opinii[64]);

- ✓ po trzecie wreszcie, informatyk może pełnić rolę audytora, a więc niezależnego eksperta prowadzącego badanie zgodności wybranych aspektów systemu informatycznego z założonymi kryteriami[65]. Audyt informatyczny jest w Polsce regulowany przepisa-

[64] Są to wysoce niekomfortowe sytuacje, bowiem wymagają od biegłego swoistego cofnięcia się w czasie. Można sobie wyobrazić, jak czułby się medyk sądowy zmuszony do oceny, czy działania podejmowane przez XVIII wiecznego znachora były zgodne z najlepszą praktyką i wiedzą dostępną w tamtym czasie i miejscu. Biorąc pod uwagę tempo rozwoju informatyki, porównanie takie nie odbiega od rzeczywistości tak bardzo, jak mogłoby się wydawać.

[65] Pojęcie audytora (w części źródeł, włącznie z niektórymi Polskimi Normami, stosuje się niepoprawną kalkę językową „auditor") bywa rozumiane w literaturze i praktyce w sposób wybitnie nieprecyzyjny. Zazwyczaj używa się go w kilku znaczeniach:

- ✓ biegłego rewidenta prowadzącego badanie ksiąg rachunkowych firmy;
- ✓ osoby prowadzącej w zasadzie dowolne badania, szczególnie badania zgodności (w tym sensie używa się pojęć takich jak „audyt legalności oprogramowania");
- ✓ audytora jednego z systemów zarządzania zgodnych ze standardami ISO.

Normami dotyczącymi audytu i audytorów są normy [ISO 19011:2011] (głównie odnośnie do audytów strony pierwszej, czyli wewnętrznych, i strony drugiej, czyli przeprowadzanych przez klientów u swoich dostawców) oraz [ISO/IEC 17021:2011] (audyty certyfikacyjne). Zob. np.: A. Gruszka: *ISO 19011:2011 Wytyczne auditowania systemów zarządzania – najważniejsze zmiany*, „Wiadomości PKN" Nr 1/2013, s. 811, http://www.pkn.pl/sites/default/files/w1_2013.pdf. Odpowiednie definicje z norm ISO brzmią:

- ✓ „audit – systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów z auditu (3.3) oraz jego obiektywnej oceny w celu określenia stopnia spełnienia kryteriów z auditu (3.2),

  UWAGA 1: Audity wewnętrzne, nazywane czasami audytami strony pierwszej, są przeprowadzane przez samą organizację lub w jej imieniu dla potrzeb przeglądu zarządzania oraz do innych celów wewnętrznych (np. w celu potwierdzenia skutecz-

mi jedynie w szczególnych przypadkach[66]. Poza nimi firma przeprowadzająca audyt może, ale nie musi, uznawać standardy dotyczące audytu (np. stosunkowo najbardziej znane standardy ISACA[67] czy IRCA[68]). Biorąc pod uwagę, że zarówno sama nomenklatura[69],

ności systemu zarządzania lub w celu uzyskania informacji dotyczących jego doskonalenia). Audity wewnętrzne mogą stanowić dla organizacji podstawę do zadeklarowania przez nią zgodności. W wielu przypadkach, w szczególności w małych organizacjach, niezależność może być wykazana przez brak odpowiedzialności za działania będące przedmiotem auditu lub przez brak uprzedzeń i konfliktu interesów,
UWAGA 2: Audity zewnętrze obejmują audity strony drugiej i audity strony trzeciej. Audity strony drugiej są przeprowadzane przez strony zainteresowane organizacją, takie jak klienci lub przez inne osoby występujące w ich imieniu. Audity strony trzeciej są przeprowadzane przez niezależne organizacje audytujące, takie jak instytucje regulacyjne lub jednostki certyfikujące,
UWAGA 3: Jeżeli co najmniej dwa systemy zarządzania z różnych dziedzin (np. jakości, środowiska, bezpieczeństwa i higieny pracy) są audytowane razem, to audit taki nazywa się audytem połączonym,
UWAGA 4: Jeżeli co najmniej dwie organizacje audytujące współpracują w celu przeprowadzenia auditu jednego auditowanego (3.7), to audit taki nazywa się auditem wspólnym,
UWAGA 5: Zaadaptowano z ISO 9000:2005, definicja 3.9.1." [PN-EN ISO 19011:2012-3.1];

- ✓ „audyt zarzadzania ryzykiem systematyczny, niezależny i udokumentowany proces pozyskiwania dowodów i obiektywnej ich oceny w celu określenia zakresu adekwatności i skuteczności struktury ramowej zarzadzania ryzykiem (2.1.1), lub jakiejkolwiek wybranej części tejże struktury" [PKN-ISO Guide 73:2012-3.8.2.6].

[66] Certyfikaty audytorów zostały wymienione w dwóch dokumentach: art. 286 ust. 1 pkt 5 ustawy o finansach publicznych (dalej UOFP) oraz w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (dalej RWCKPIST).

[67] Ang. *Information Systems Audit & Control Association*. Według definicji ISACA „Audyt systemów informatycznych, to proces zbierania i oceniania dowodów w celu określenia, czy systemy informatyczne i związane z nimi zasoby właściwie chronią majątek, utrzymują integralność danych i systemu, dostarczają odpowiednich i rzetelnych informacji, osiągają efektywnie cele organizacji, oszczędnie wykorzystują zasoby i stosują mechanizmy kontroli wewnętrznej tak, aby dostarczyć rozsądnego zapewnienia, że są osiągane cele operacyjne i kontrolne oraz że chroni się przed niepożądanymi zdarzeniami lub są one na czas wykrywane, a ich skutki korygowane" (za: M. Forystek: *Audyt informatyczny*, InforAudit, Warszawa 2005).

[68] Ang. *International Register of Certificated Auditors*.

jak i idące za nią rozwiązania biznesowe i techniczne są obecnie w fazie dynamicznego rozwoju, trudno formułować jakiekolwiek spostrzeżenia metodologiczne natury bardziej ogólnej. Warto pamiętać, że – przynajmniej jeśli mowa o audycie, tak jak jest on rozumiany w znaczeniu audytu systemów zarządzania na zgodność z normami ISO – na dowód audytowy nałożone są inne ograniczenia niż na dowód w sensie prawnym i jeszcze inne niż na dowód w sensie naukowym. Metody pracy audytora to przede wszystkim obserwacja, analiza dokumentów oraz wywiady, wysnuwane przezeń wnioski dotyczą zgodności pomiędzy twierdzeniami (o danych ekonomicznych, systemie zarządzania) i ustanowionymi kryteriami (normami ISO, przepisami prawa itd.), zaś samo badanie ma charakter wysoce fragmentaryczny[70]. Stąd wnioski będące rezultatem audytu mogą mieć charakter stanowczy praktycznie wyłącznie wtedy, jeśli są to wnioski negatywne (np. „system zarządzania bezpieczeństwem informacji nie jest zgodny z wymaganiami zawartymi w normie ISO/IEC 27001, bowiem stwierdzono poważną niezgodność z wymaganiami normy"), natomiast wnioski pozytywne wobec ograniczenia metod i zakresu badania są co najwyżej wnioskami uprawdopodabniającymi[71].

Zarysowane wyżej schematycznie role są przykładami działalności opiniodawczej, przy czym każda z nich podlega specyficznym warunkom i ograniczeniom. Opiniowanie sądowe jest, w tym ujęciu, szczególnym przykładem działalności rzeczoznawczej, posiadającym własną specyfikę i uwarunkowania, której to specyfice i uwarunkowaniom poświęcona jest ta monografia.

[69] Zob. np.: K. Liderman: *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?*, „Biuletyn Instytutu Automatyki i Robotyki" Nr 21/2004, WAT, Warszawa 2004; M. Forystek: *Audyt*…, op. cit., s. 25.

[70] Zob. np.: M. Molski, M. Łacheta: *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007, s. 155 i nast.

[71] Badania prowadzone w ramach audytu są zawsze wyrywkowe, a więc niestwierdzenie zaistnienia jakiegoś faktu nie jest równoważne stwierdzeniu jego niezaistnienia (w ogóle w obrębie badanego systemu).

2.3 Pojęcie biegłego sądowego

Pojęcia biegłego sądowego nie definiuje i nie definiował w przeszłości żaden z polskich przepisów proceduralnych ani żaden z licznych pozakodeksowych aktów prawnych, dopuszczających możliwość powoływania biegłych[72]. Zazwyczaj przyjmuje się, zgodnie z wykładnią językową, że biegły jest osobą posiadającą wiedzę fachową i doświadczenie w jakiejś dziedzinie[73]. Biegły sądowy jest organem pomocniczym sądu w wypadkach wymagających wiadomości specjalnych[74].

Pojęcie „wiadomości specjalnych" nie jest również zdefiniowane w aktach prawnych. Sąd Najwyższy w jednym z wyroków[75] określił je w sposób następujący:

„Wiadomości specjalne to szczególna wiedza specjalistyczna z danej dziedziny sztuki, techniki, kultury, budownictwa, przemysłu, rolnictwa, transportu, komunikacji, informatyki, chemii etc., obejmująca wiadomości wykraczające poza zakres tych, jakimi dysponuje ogół osób inteligentnych i ogólnie wykształconych".

Rozporządzenie Ministra Sprawiedliwości z 24 grudnia 1928 r. o biegłych sądowych (dalej RoBS) wprowadziło podział biegłych na dwie grupy: tzw. biegłych sądowych z listy oraz spoza listy (zwanych też „biegłymi *ad hoc*"). Pierwsi ustanawiani są przez prezesów sądów okręgowych i wpisywani na listę biegłych, z której korzystają organy wymiaru sprawiedliwości, drudzy – jednorazowo powoływani do poszczególnych spraw.

2.3.1 Ustanawianie biegłych

Zasady ustanawiania biegłych z listy reguluje obecnie rozporządzenie Ministra Sprawiedliwości z 24 stycznia 2005 r. w sprawie biegłych sądowych (dalej RwsBS). Zgodnie z tym rozporządzeniem biegłych sądowych ustana-

[72] W książce A. Kegel, Z. Kegel: *Przepisy o biegłych sądowych, tłumaczach i specjalistach. Komentarz*, Zakamycze, Kraków 2004, s. 14–28, wymieniono *explicite* 22 pozakodeksowe akty prawne regulujące różne aspekty opiniowania sądowego, co oczywiście nie wyczerpuje całego katalogu.

[73] Część prawników i teoretyków prawa zwraca uwagę, że biegły – oprócz odpowiedniej wiedzy fachowej – powinien posiadać odpowiednią praktykę zawodową (zob. ibid., s. 30 i nast.).

[74] Zob. wyrok Naczelnego Sądu Administracyjnego z 4 czerwca 2001 r. (II SA 1434/00).

[75] Wyrok Sądu Najwyższego z 18 lipca 1975 r. (I CR 331/75).

wia przy Sądzie Okręgowym prezes tego sądu na okres 5 lat. Biegłym może być ustanowiona osoba, która korzysta z pełni praw cywilnych i obywatelskich, ukończyła 25 lat życia, posiada teoretyczne i praktyczne wiadomości specjalne w danej gałęzi nauki, techniki, sztuki, rzemiosła, a także innej umiejętności, dla której ma być ustanowiona, daje rękojmię należytego wykonywania obowiązków biegłego i wyrazi zgodę na ustanowienie jej biegłym. Ustanowienie biegłym osoby zatrudnionej wymaga zasięgnięcia opinii zakładu pracy zatrudniającego tę osobę, zaś ustanowienie biegłym osoby wykonującej wolny zawód wymaga zasięgnięcia opinii organizacji zawodowej, do której osoba ta należy. Posiadanie wiadomości specjalnych powinno być wykazane dokumentami lub innymi dowodami. Ocena, czy posiadanie wiadomości specjalnych zostało dostatecznie wykazane, należy do Prezesa Sądu Okręgowego.

Choć wydaje się to dziwne, inaczej wygląda w różnych Sądach Okręgowych praktyka powoływania biegłych i korzystania z ich opinii. Obecnie w Polsce istnieje 45 okręgów sądowych, których prezesi powołują biegłych. W Biuletynie Informacji Publicznej poszczególnych sądów zamieszczone są informacje dotyczące zestawu dokumentów, jakie wymagane są od kandydata na biegłego. Zestawy te są różne dla różnych sądów. I tak np. Sąd Okręgowy w Białymstoku jako dokumenty, które powinien złożyć kandydat na biegłego podaje 11 dokumentów[76]:

1) wniosek skierowany do Prezesa Sądu Okręgowego w Białymstoku o ustanowienie biegłym sądowym (należy określić dziedzinę);
2) życiorys/CV;
3) kwestionariusz osobowy;
4) kserokopia dowodu tożsamości;
5) odpis dyplomu ukończenia studiów wyższych;
6) inne dokumenty potwierdzające posiadanie szczególnych kwalifikacji zawodowych oraz praktycznych i teoretycznych wiadomości specjalnych z dziedziny, w której osoba ubiega się o ustanowienie biegłym, gdy wniosek składa lekarz powinien mieć I lub II stopień specjalizacji;
7) opinia i zgoda zakładu pracy;

[76] Zob. http://bialystok.so.gov.pl/informacje/biegli.html.

8) opinia organizacji zawodowej działającej na podstawie ustawy z 7 kwietnia 1989 r. – prawo o stowarzyszeniach (Dz.U. z 2001 r. Nr 79, poz. 855) bądź na podstawie innych ustaw (w przypadku lekarza opinia Okręgowej Izby Lekarskiej);

9) oświadczenie kandydata, że nie jest przeciwko niemu prowadzone postępowanie o przestępstwo ścigane z oskarżenia publicznego lub przestępstwo skarbowe;

10) oświadczenie o korzystaniu z pełni praw cywilnych i obywatelskich;

11) opłata skarbowa w wysokości 10 zł na konto Urzędu Miejskiego w Białymstoku departament finansów miasta.

Podczas gdy w Sądzie Okręgowym w Bielsku-Białej kandydat na biegłego musi przedstawić 14 dokumentów[77]:

1) wniosek (adresowany do Prezesa Sądu Okręgowego w Bielsku-Białej) o ustanowienie biegłym sądowym przy Sądzie Okręgowym w Bielsku-Białej z zaznaczeniem gałęzi nauki, techniki, sztuki, rzemiosła, a także innej umiejętności, dla której posiada teoretyczne i praktyczne wiadomości specjalne;

2) życiorys (CV);

3) kwestionariusz osobowy;

4) odpis dyplomu oraz inne dokumenty potwierdzające posiadanie teoretycznych i praktycznych wiadomości specjalnych w danej dziedzinie;

5) w przypadku lekarzy: odpis dyplomu lekarskiego, prawo wykonywania zawodu lekarza, zaświadczenie o uzyskaniu specjalizacji;

6) opinię z ostatniego miejsca pracy (dotyczy to osoby zatrudnionej), bądź organizacji zawodowej (od osoby wykonującej wolny zawód);

7) kserokopię dowodu osobistego;

8) aktualne zapytanie o karalność z Krajowego Rejestru Karnego;

9) oświadczenie o korzystaniu z pełni praw cywilnych i obywatelskich;

10) oświadczenie, że aktualnie nie toczy się postępowanie przygotowawcze, jak też sądowe postępowanie karne;

[77] Zob. http://www.bielsko-biala.so.gov.pl/biegli-sadowi,m,mg,3,24.

11) oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych;

12) zobowiązanie o niezwłocznym powiadomieniu Prezesa Sądu Okręgowego w Bielsku-Białej o wszczętym postępowaniu karnym przeciwko biegłemu;

13) pisemną zgodę na pełnienie funkcji biegłego sądowego;

14) zdjęcie.

W obu tych zestawach występują elementy zgoła kuriozalne: oświadczenie o wyrażeniu zgody na przetwarzanie danych osobowych (załączony na stronach BIP formularz nie precyzuje ani zakresu zgody, ani nawet tego, komu taka zgoda jest udzielana, nie mówiąc już o tym, że sąd ma prawo przetwarzać dane osobowe biegłych, bez konieczności uzyskiwania takiej zgody), potwierdzenie wpłaty na konto urzędu miejskiego (a więc jednostki organizacyjnej gminy – urzędu administracji nawet nie państwowej, ale samorządowej), oświadczenie, że aktualnie nie toczy się postępowanie przygotowawcze (jak można się domyślić z kandydatem na biegłego w roli podejrzanego, choć formalnie rzecz ujmując podejrzanym jest osoba, wobec której wydano postanowienie o przedstawieniu zarzutów albo której bez wydania takiego postanowienia postawiono zarzut w związku z rozpoczęciem przesłuchania w charakterze podejrzanego, a nie osoba, której takie postanowienie przedstawiono, potencjalny kandydat na biegłego nie musi, w szczególnym przypadku, wiedzieć, że postanowienie takie zostało podjęte), czy zdjęcie (trudno domyślić się podstawy prawnej takiego żądania). Inne sądy okręgowe precyzują zazwyczaj mniejsze wymagania, przy czym z powołanych przepisów zdaje się wynikać możliwość wymagania wniosku o ustanowienie biegłym sądowym, kwestionariusza osobowego bądź życiorysu, dokumentów potwierdzających znajomość dziedziny i posiadanie kwalifikacji zawodowych oraz opinii[78] zakładu pracy zatrudniającego tę osobę lub organizacji zawodowej.

[78] Opinii, a nie zgody (por. § 3 RwsBS). Trudno wyobrazić sobie, żeby prezes Sądu Okręgowego przy podjęciu decyzji o wpisaniu na listę biegłych osoby, która chce zostać biegłym i która w jego mniemaniu spełnia wszystkie wymagane warunki merytoryczne, był związany decyzją kierownika zakładu pracy, w którym kandydat na biegłego jest zatrudniony, pomijając już fakt, że wśród biegłych znajdują się osoby zarówno pracujące we własnych

Wymóg dostarczenia odpowiedzi na zapytanie do Krajowego Rejestru Karnego wiąże się z koniecznością poniesienia przez kandydata na biegłego kosztów (jest to bowiem dokument wydawany odpłatnie). Nie jest on natomiast dokumentem poświadczającym wymaganą w powołanym rozporządzeniu[79] pełnię praw cywilnych i obywatelskich ani – tym mniej – wystarczający do uznania, że osoba daje rękojmię należytego wykonywania obowiązków biegłego[80]. Choć niewątpliwie niekaralność jest tej rękojmi warunkiem koniecznym, to nie jest warunkiem wystarczającym. Być może dałoby się obowiązek wylegitymowania się przez kandydata na biegłego niekaralnością w jakiś sposób z przepisów wywieść (jakkolwiek nie bardzo wiadomo dlaczego koszt tego obowiązku ma obciążać kandydata na biegłego).

2.3.2 Odpowiedzialność biegłego

W czasie sprawowania funkcji biegłego sądowego konieczne jest zwrócenie uwagi na kilka, nie zawsze intuicyjnie zrozumiałych, uwarunkowań i ograniczeń.

Bardzo mocno podkreślaną w orzecznictwie i praktyce kwestią jest bezwzględny zakaz używania tytułu biegłego sądowego (oczywiście dotyczy to również biegłych „z listy") w innych działaniach, tj. poza opiniami na zlecenie uprawnionych podmiotów. Takie użycie tytułu jest działaniem bezprawnym i – jak orzekł Naczelny Sąd Administracyjny[81] – dyskredytuje daną osobę w stopniu pozwalającym uznać, iż nie daje ona rękojmi należytego wykonywania obowiązków biegłego[82]. Niektóre skrajnie rygorystyczne sądy zabraniają używania przez osoby wpisane na listę biegłych słów „biegły sądowy" nawet na wizytówkach czy w biogramach. Biorąc pod uwagę, że fakt bycia wpisanym na listę biegłych sądowych nie jest w żaden sposób informacją niejawną, można tylko zalecić biegłym z takich okręgów

firmach, jak i pracujące w więcej niż jednym miejscu, wymóg ten wydaje się więc nieco archaiczny.

[79] Por. §12 ust. 1 pkt 1. RwsBS.

[80] Por. §12 ust. 1 pkt 4. RwsBS.

[81] Zob. wyrok Naczelnego Sądu Administracyjnego z 4 czerwca 2001 r. (II SA 1434/00).

[82] Por. postanowienie Sądu Najwyższego z 22 kwietnia 1996 r. (I PRN 30/96); orzeczenie Naczelnego Sądu Administracyjnego z 20 sierpnia1998 r. (II SA 992/98).

używanie form opisowych (np. „został wpisany na listę biegłych sądowych w Sądzie Okręgowym w …").

Za wydaną opinię biegły ponosi odpowiedzialność zarówno karną, jak i cywilną. Można mówić również o pewnej formie odpowiedzialności dyscyplinarnej biegłych sądowych[83] wpisanych na listę biegłych sądowych: Prezes Sądu Okręgowego może zwolnić z funkcji biegłego z ważnych powodów, a w szczególności, jeżeli nienależycie wykonuje on swoje czynności[84], jak również biegły, co do którego powstały wątpliwości odnośnie do tego, czy daje gwarancję należytego wykonywania obowiązków biegłego sądowego, może liczyć się z niepowołaniem na kolejną kadencję. W tym kontekście można mówić o sumienności w wykonywaniu obowiązków biegłego (m.in. o obowiązku terminowego sporządzania opinii i usprawiedliwiania przyczyn opóźnień)[85].

Odpowiedzialność karna z art. 233 Kodeksu karnego (dalej KK) ma miejsce wtedy, gdy biegły dopuścił się tzw. fałszu intelektualnego[86] w wydanej opinii (ustnej lub pisemnej), natomiast możliwa jest także odpowiedzialność z art. 271 § 1 KK[87]. Zdecydowanie należy – podobnie zresztą jak wszędzie, gdzie mowa o odpowiedzialności karnej za wypowiedzi – odróżnić poświadczenie faktów od wyrażonych przez biegłego

[83] Zob. M. Bojarski: *Problemy odpowiedzialności karnej i dyscyplinarnej biegłego*, „Jurisprudencija" T. 18(10)/2000, s. 24–28.

[84] Zob. § 6 ust. 1 pkt 2 RwsBS.

[85] Zob. wyrok Naczelnego Sądu Administracyjnego z 27 maja 2009 r. (II GSK 971/08).

[86] Wyrok Sądu Najwyższego z 7 grudnia 2001 r. (IV KKN 563/97): „Odpowiedzialność karna biegłego za przestępstwo tzw. fałszu intelektualnego dotyczy poświadczenia faktów, które poddają się weryfikacji z punktu widzenia ich prawdziwości lub fałszu, natomiast nie obejmuje samych ocen".

[87] Wyrok Sądu Najwyższego (IV KKN 563/97): „Biegły sądowy lub rzeczoznawca, z racji pełnionej funkcji i posiadanych uprawnień, nie działa we własnym imieniu i we własnej sprawie, a w sytuacji, gdy wydaje on opinię, co najmniej godząc się z jej nierzetelnością, tym samym poświadcza w niej nieprawdę co do okoliczności mającej znaczenie prawne. Może więc być podmiotem przestępstwa określonego w art. 271 § 1 KK (art. 266 § 1 KK z 1969 r. KK), jeżeli swoim zachowaniem wyczerpuje jego znamiona, a jednocześnie nie bierze bezpośredniego udziału w postępowaniu sądowym lub w innym postępowaniu prowadzonym na podstawie ustawy".

ocen. W tym sensie trudno zgodzić się np. z Karolem Pachnikiem[88], który pisze:

„Zagadnienie fałszywej opinii wystąpi w sytuacjach:

- ✓ gdy ocena formułowana w opinii będzie wyraźnie sprzeczna z aktualnym stanem wiedzy w dziedzinie, której opinia dotyczy;
- ✓ gdy ocena formułowana w opinii będzie wyraźnie sprzeczna z rzeczywistym stanem faktycznym, możliwym do wyinterpretowania z akt sprawy;
- ✓ gdy ocena będzie oparta na wyraźnie błędnej metodzie badawczej.

Istotną okolicznością jest, że ocena musi być też od strony subiektywnej (świadomie) nieprawdziwa, a ów element świadomości zachodzić będzie we wszystkich wskazanych sytuacjach".

Zapewne wystąpiło tu pomylenie oceny z opinią (skądinąd słusznie wskazuje się w literaturze przedmiotu, że lepszym sformułowaniem, niestety nieużytym przez ustawodawcę, na określenie opinii, byłaby „ekspertyza" – zob. rozdział 3).

Biegły może ponieść odpowiedzialność karną oczywiście również za inne czyny, znamiona, których może wyczerpać formułując opinię (ustną lub pisemną), np. za pomówienie osoby o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności.

Odpowiedzialność cywilna biegłych jest zagadnieniem stosunkowo nowym[89], można o niej mówić co najmniej w dwu kontekstach: odpowie-

[88] Zob. K. Pachnik: *Prawne uwarunkowania odpowiedzialności cywilnej i karnej biegłych w polskim systemie prawnym*, „Edukacja Prawnicza" Nr 10 (118)/ 2010, http://www.edukacjaprawnicza.pl/artykuly/artykul/a/pokaz/c/artykul/art/prawne-uwarunkowania-odpowiedzialnosci-cywilnej-i-karnej-bieglych-w-polskim-systemie-prawnym.html.

[89] Zob. uchwała Naczelnego Sądu Administracyjnego z 12 stycznia 2009 r. (I FPS 3/08): „biegły odpowiada osobiście za wykonane przez siebie czynności niezależnie od tego, czy do określonych działań zobowiązał go sąd, czy też inny organ. W wyniku zlecenia wydania opinii nie dochodzi do przeniesienia odpowiedzialności za wynik działania biegłego sądowego na sąd lub inny organ" oraz wyrok Trybunału Konstytucyjnego z 12 czerwca 2008 r. (K 50/05): „Biegły odpowiada osobiście za wykonywane przez siebie czynności, niezależnie od tego, czy do określonego działania zobowiązał go sąd, czy też inny organ. Sam fakt, iż wydanie opinii zleca sąd, czy też inny organ, nie oznacza, że to on przyjmuje odpowiedzialność wobec osób trzecich. Opinia wydana przez biegłego jest dowodem w postępowaniu

działności za decyzje podejmowane w postępowaniach z wykorzystaniem opinii biegłego, który przyczynił się do skłonienia organu procesowego do podjęcia określonej decyzji[90] oraz o odpowiedzialność wobec osób trzecich za szkody powstałe w związku z wykonywaniem funkcji biegłego[91].

sądowym, podlegającym ocenie na równi z innymi dowodami, a nie usługą, której bezpośrednim odbiorcą jest uczestnik postępowania. Sąd ponosi odpowiedzialność jedynie za swoje rozstrzygnięcie, wydane w oparciu o ocenę wszystkich okoliczności w sprawie, w tym także tych, które wymagają wiadomości specjalnych, ale nie za czynności biegłego. Sąd, powołując biegłego z listy biegłych w celu wydania ekspertyzy, odwołuje się do jego specjalistycznej wiedzy, stąd wydana w oparciu o tę wiedzę opinia musi być w pełni samodzielna. Na samodzielność w wydaniu opinii, rozumianej jako wyrażanie własnych poglądów biegłego w danej sprawie, nie wpływa fakt, iż biegły ma obowiązek stosować się do wskazówek organu zlecającego, np. co do zakresu opinii. To, że biegły sporządza opinię w oparciu o akta sprawy przekazane przez zlecającego, nie może przesądzać o tym, iż nie jest on samodzielny. Nie dochodzi do przeniesienia na sąd odpowiedzialności za wyniki działań biegłego sądowego".

[90] Por. K. Pachnik: *Prawne*…, op. cit. Autor słusznie zauważa, że „Zaznaczyć trzeba, że czyn biegłego musi być bezprawny. Bezprawność – jako przedmiotowa cecha czynu sprawcy – tradycyjnie ujmowana jest jako sprzeczność z obowiązującym porządkiem prawnym. Pojęcie »porządek prawny« obejmuje przy tym nakazy i zakazy wynikające z normy prawnej, lecz także nakazy i zakazy wynikające z norm moralnych i obyczajowych (…). Przy tym wedle orzecznictwa sam fakt sporządzenia przez biegłych opinii na polecenie sądu nie usuwa ewentualnej bezprawności ich działania, polegającej na nierzetelnym wykonaniu obowiązków biegłych".

[91] K. Pachnik zauważa, że „Unormowania takie w ogólności charakteryzują się ograniczeniem do odpowiedzialności z tytułu czynów niedozwolonych" (K. Pachnik: *Prawne*…, op. cit.); bardziej natomiast zdecydowane stanowisko prezentuje T. Widła (zob. T. Widła: *Glosa do wyroku TK RP z 12 czerwca 2008 r. [K 50/05]*, „Palestra" Nr 78/2008, s. 291–301; T. Widła: *VAT-em biegłych, wystąpienie na 1. Kongresie Nauk Sądowych*, http://www.ptrm.pl/praktyka/warsztat-wyceny/informacja-z-przebiegu-pierwszego-kongresu-nauk-sadowych-w-warszawie), który postuluje daleko idącą ostrożność, zalecając biegłym m.in. „(…) Bez jednoznacznego wskazania w postanowieniu (przez zaznaczenie, że organ procesowy zleca te czynności na własną odpowiedzialność) nie podejmować żadnych czynności badawczych, które mogłyby łączyć się ze zniszczeniem, uszkodzeniem, a nawet jakimkolwiek pomniejszeniem wartości (rynkowej, emocjonalnej) badanego przedmiotu (…). Unikać wydawania tzw. opinii kategorycznych (w efekcie rozstrzygnięcie kwestii odpowiedzialność – spadnie wyłącznie na organ procesowy)". Z metodologicznego punktu widzenia takie stawianie sprawy może budzić wątpliwości. Wątpliwości może budzić odpowiedzialność biegłych za domniemane naruszenie dóbr osobistych osoby, odnośnie do której wydawana jest opinia. Wyrokiem z 11 maja 2005 r. Sąd Apelacyjny w Poznaniu (I ACa 1875/04) prawomocnie oddalił powództwo, w którym powód domagał się łącznie zadośćuczynienia od biegłych psy-

Z punktu widzenia biegłego informatyka na szczególną uwagę zasługują odpowiednio trzy sytuacje:

- ✓ prowadzenie badań niszczących, w informatyce związane przede wszystkim z badaniem zawartości pamięci ulotnej urządzeń (w szczególności takich jak telefony komórkowe);
- ✓ uzyskiwanie dostępu do informacji chronionej, związanego z przełamywaniem jej ewentualnych zabezpieczeń;
- ✓ wykonywania czynności wykraczających poza zakres opinii.

W pierwszych dwóch przypadkach wskazane może być uzyskanie jasno sprecyzowanego polecenia wydanego w formie postanowienia organu procesowego[92]; sytuacji trzeciej należy zdecydowanie unikać[93].

chiatrów za użycie w treści ich opinii psychiatrycznej, wytworzonej na potrzeby jednej ze spraw toczących się przed Sądem Rejonowym twierdzeń, które naruszały jego dobre imię. Sąd stwierdził, że „(…) Jeżeli opinia biegłych zawiera wprawdzie oceny stanu psychicznego uczestnika procesu, które mogły naruszać jego dobra osobiste, jednak wydana została w granicach działań prawnych, na polecenie sądu, sporządzona została z wykorzystaniem wskazanego przez ten sąd materiału, rzetelnie wskazywała na niedostatki bazy diagnostycznej, zawierała oszczędne sformułowania i wnioski, to nie można jej uznać za bezprawną", zauważył jednak również, że „Sam fakt sporządzenia przez biegłych opinii na polecenie sądu nie usuwa ewentualnej bezprawności ich działania, polegającej na nierzetelnym wykonaniu obowiązków biegłych".

[92] Warto pamiętać, że badania informatyczne dotyczą nie tylko komputerów będących narzędziem przestępstwa, ale również urządzeń należących do świadków, poszkodowanych czy stron w procesie cywilnym. Jeśli wydanie opinii wiązałoby się z potencjalnym uzyskaniem przez osoby (np. publiczność na sali sądowej) postronne informacji, których ujawnienie mogłyby być dla stron niepożądane, biegły powinien poinformować o tym organ procesowy i uzyskać odpowiednie postanowienie, w którym *explicite* zawarte będzie polecenie np. przełamania zabezpieczeń czy ujawnienia wszystkich treści znajdujących się na nośniku.

[93] Z praktyki autora można przytoczyć sytuację, w której biegły informatyk wykonując opinię dotyczącą zupełnie innej okoliczności, dołączył do niej kilkaset stron zawierających wydruki wpisów *cookies* przeglądarki internetowej, a w czasie rozprawy zaczął komentować zachowanie powoda, który jego zdaniem często odwiedzał strony pornograficzne (co dziwne, informatyk nie zwrócił uwagi na liczbę odwiedzin i średni czas przebywania na tych stronach, które sugerowały, że przeglądarka padła ofiarą złośliwego programu typu *jumper*. Biegły nie sprawdził zresztą badanego nośnika na obecność wirusów i *malware*). Posiadacz badanego komputera wytoczył biegłemu proces o naruszenie dóbr osobistych (w tej sytuacji mógł zresztą również złożyć doniesienie do prokuratury o składanie fałszywych zeznań i wytoczyć proces karny o zniesławienie).

Odpowiedzialność cywilna może dotyczyć również przypadkowego uszkodzenia sprzętu w trakcie badań. Jest to zagadnienie o tyle trudne, że przeważnie niemożliwe jest dokładne ustalenie momentu awarii urządzenia elektronicznego (a wiec tego, czy doszło do niej np. w trakcie procesowego zabezpieczania komputera przez policję, czy w magazynie prokuratury, czy podczas badania przez biegłego), ponadto należałoby rozróżnić uszkodzenie, do jakiego mogło dojść przypadkowo (na skutek działania czynników losowych, niemożliwych do przewidzenia), od uszkodzenia będącego skutkiem błędu biegłego.

2.4 Biegły jako narzędzie sądu

Rola biegłych w procesie bywała rozumiana na cztery sposoby:

- ✓ sędziów faktów (łac. *iudici facti*)[94],
- ✓ uczonych świadka[95] (ang. *expert witness*),
- ✓ źródeł dowodowych[96],
- ✓ narzędzi sądu[97].

Współcześnie zarówno procesualiści, jak i sami biegli, uznają za trafne (w systemie prawa polskiego) jedynie dwa ostatnie punkty widzenia. W trakcie czynności procesowych biegły jest traktowany jako źródło dowodowe (dostarcza środka dowodowego, jakim jest opinia: „dowód z opinii biegłego") lub też może być konsultantem organu procesowego, uczestnicząc w czynnościach przez ten organ prowadzonych (w szczególności przy zabezpieczaniu materiału dowodowego, uczestnicząc w przesłuchaniu świadków i stron, a także w oględzinach i eksperymentach procesowych), udzielając porad i wskazówek[98]. Nie oznacza to bynajmniej deprecjonowania roli biegłego, wręcz przeciwnie – jednym z najczęściej

[94] Jest to podejście wywodzące się z tradycji prawa niemieckiego (zob. np.: A. Kegel, Z. Kegel: *Przepisy*…, op. cit., s. 34 i nast.; J. Turek: *Biegły sądowy i jego czynności*, „Monitor Prawniczy" Nr 24/2007, s. 1358-1364).

[95] Tego rodzaju podejście (ang. *expert-witness*) funkcjonuje w systemie prawa USA. Por. np. T. Widła: *Uwagi o przeprowadzaniu dowodu z opinii biegłych*, „Palestra" Nr 34/2002, s. 66–73; Z. Marek: *Wybrane*…, op. cit., s. 241.

[96] Zob. A. Kegel, Z. Kegel: *Przepisy*…, op. cit., s. 35 i nast.

[97] Zob. np.: J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 25 i nast.

[98] Zob. przypis 97.

wysuwanych pod adresem biegłych zarzutów jest ich nadmierna rola w trakcie procesu, w którym – wobec braku wiadomości specjalnych organu procesowego – dowód z opinii biegłego ma decydujące znaczenie.

Zagadnieniu opiniowania sądowo-informatycznego poświęcona jest druga część książki, poniżej natomiast zostaną pokrótce omówione zadania biegłego informatyka, w których występuje on jako narzędzie organu procesowego.

2.4.1 Udział biegłego informatyka w zabezpieczaniu materiału dowodowego

Zabezpieczanie materiału dowodowego odbywa się zazwyczaj w postępowaniu przygotowawczym w sprawach karnych – art. 297 § 1 pkt 5 Kodeksu postępowania karnego (dalej KPK); zdarza się jednak, że dochodzi do niego również w postępowaniu sądowym. Możliwe jest też zabezpieczenie dowodów w postępowaniu cywilnym – zob. rozdział 3 Kodeksu postępowania cywilnego (dalej KPC)[99]. Samo zabezpieczenie sprzętu komputerowego powinno być wykonywane przez osobę dysponującą odpowiednimi wiadomościami specjalnymi z zakresu informatyki, jedną bowiem z najważniejszych cech tzw. dowodów elektronicznych jest ich nietrwałość: niewłaściwe postępowanie z materiałem badawczym może prowadzić do jego kontaminacji (zanieczyszczenia), w szczególności do zmiany zapisów umieszczonych na nośniku, w tym zarówno treści dokumentów elektronicznych, jak i metadanych[100].

Już samo włączenie komputera powoduje zmiany w logach systemowych, a zatem narusza integralność zapisanych w nich informacji, co uznaje się za kontaminację materiału dowodowego, niekiedy tak znaczną, że uniemożliwiającą wydawanie na jego podstawie opinii sądowych[101]. Z tego

[99] Zabezpieczenie dowodu w postępowaniu cywilnym polega na przeprowadzeniu dowodów przed wszczęciem postępowania lub w jego toku, lecz wcześniej niż przy normalnym przebiegu postępowania dowodowego.

[100] Metainformacja (metadane) to „informacja o informacji", np. o dacie napisania danego dokumentu tekstowego, czasie ostatniego dostępu do niego itd.

[101] W polskim prawie nie funkcjonuje wprawdzie formalna teoria dowodowa, a w szczególności zasada „owoców zatrutego drzewa", niemniej może zdarzyć się, że stan materiału dowodowego przekazanego do badań uniemożliwi wydanie opinii o jakimkolwiek stopniu stanowczości wniosków, co w praktyce czyni materiał dowodowy nieprzydatnym. Można tu przytoczyć przypadek (opisany w artykule M. Szmit: *Z całą sumiennością i bezstronnością,*

też względu, w przypadku analizy sądowo-informatycznej informatycznych nośników danych niezbędne jest korzystanie z mechanizmów sprzętowych lub programowych, zabezpieczających badany nośnik przed modyfikacją (tzw. blokerów zapisu). W przypadku standardowych dysków stosuje się zazwyczaj blokery sprzętowe, a w przypadku dysków z niestandardowymi interfejsami (np. dysków SSD wlutowanych w płytę komputera) – blokery programowe. Prawidłowy sposób procesowego zabezpieczenia cyfrowych nośników informacji oraz prowadzenia ich analizy wykracza poza tematykę tej monografii[102]. Na pewno należy pamiętać o odpowied-

czyli o informatyce sądowej, „Magazyn Informatyki Śledczej" Nr 7/2010, s. 46, http://www.mediarecovery.pl/magazyn-is/magazyn_is_numer_7.pdf), w którym prokuratura dostarczyła do badania komputer oraz akta śledztwa, w których, oprócz informacji o dacie i godzinie przeszukania i zatrzymania rzeczy, znajdował się m.in. protokół oględzin, z którego wynikało, że komputer był poddany – w kilka miesięcy po zatrzymaniu – trwającym godzinę oględzinom wykonanym przez specjalistę policyjnego. W protokole nie zapisano, na czym owe oględziny polegały. Z analizy logów w komputerze wynikało, że komputer był od chwili policyjnego przeszukania uruchamiany kilkukrotnie w kolejnych dniach. Policyjny „specjalista" za pomocą hakerskiego oprogramowania, (pracując „na żywca", czyli na zabezpieczonym – choć to słowo już nie bardzo tu pasuje – sprzęcie) wyzerował hasła użytkowników, następnie zalogował się na poszczególne konta, przeglądając z nich różne pliki i uruchamiając różne programy. Efektem tych działań było oczywiście zamazanie części historii użytkowania komputera, zmiany czasów MAC, zawartości pamięci wirtualnej itd. W tej sytuacji wydanie opinii było niemożliwe z powodu zerwania ciągłości łańcucha dowodowego przez nieudokumentowane operacje na nośniku, wprowadzenie szeregu zmian danych zapisanych na nośniku i znaczne zanieczyszczenie materiał badawczego. Dodatkowo osoba prowadząca oględziny wykazała się nie tylko skrajnym brakiem wiedzy, ale i prawdopodobnie dopuściła się czynów karalnych, fałszując dokumenty śledztwa (w protokole oględzin podano nieprawdziwe informacje na temat czasu i liczby uruchomień komputera). Wobec tego nie można było w sposób uzasadniony przypuszczać, że pozostałe znajdujące się na nośniku treści są tożsame z treściami znajdującymi się na nim w chwili zabezpieczenia materiału dowodowego. Stan materiału dowodowego przekazanego do badań uniemożliwiał wydanie opinii, zadaniem biegłego nie jest bowiem dywagowanie na temat ewentualnych możliwych sytuacji, ale poinformowanie gospodarza postępowania o istniejącym stanie rzeczy.

[102] W załączniku zamieszczono rekomendacje dotyczące zabezpieczenia dysków twardych opracowane przez Sekcję Informatyki Sądowej Polskiego Towarzystwa Informatycznego w 2009 r. Warto również zapoznać się z normą [ISO/IEC 27037:2012], przy czym należy pamiętać, że systemy prawne poszczególnych krajów mogą implikować tryb postępowania z materiałem dowodowym. Zob. też: J. Meteňko: *Možnosti A Využívanie KAI Technológii Pri*

nim zaplanowaniu czynności (włącznie z oszacowaniem ile i jakiego rodzaju urządzeń będzie w czasie zabezpieczenia potrzebnych[103], jaki może być szacunkowy czas trwania czynności, czy i kiedy w trakcie zabezpieczenia należy zdecydować o odłączeniu urządzeń od sieci komputerowych[104]) i o konieczności dokumentowania zastanego stanu (np. jakie urządzenie w jaki sposób było połączone z innymi, włącznie z wykonaniem fotografii) i podjętych działań. Warto zaznaczać, że podstawową zasadą jest wykonanie kopii binarnej nośnika i prowadzenie badań na niej[105], co – w przypadku współczesnych dysków twardych o pojemnościach rzędu terabajtów – może trwać nawet kilkanaście godzin[106]. Z tego powodu w miarę możli-

Kontrole Závažnej Kriminality, „Securitologia" Nr 6/2007, s. 112–118; J. Meteňko: *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*, Akademia PZ, Bratislava 2005.

[103] Na przykład jeśli badanie ma być prowadzone w trybie *live* trzeba zapewnić odpowiednią ilość nośników, na których zostaną zapisane wyniki (ewentualnie, na które będzie wykonana kopia nośników oryginalnych), jeśli w czasie badania grozić będzie utrata zasilania (a więc związane z tym konsekwencje w postaci wyłączenia i unieruchomienia sprzętu), należy zadbać o odpowiednie zasilanie awaryjne itd.

[104] Chodzi zarówno o kwestie takie jak uniemożliwienie ewentualnego zdalnego dostępu, o wpływ odłączenia od sieci na działające programy, jak i wreszcie o tryb synchronizacji zegarów systemowych z czasem sieciowym: weryfikacja zgodności czasu wskazywanego przez urządzenie z czasem rzeczywistym ma bowiem kluczowe znaczenie w przypadku analizy metadanych obejmujących czasy ostatniej modyfikacji, ostatniego dostępu do pliku i jego utworzenia (tzw. czasy MAC, ang. *Modification, Access, Creation*).

[105] Nieco inne postępowanie może mieć miejsce w przypadkach, gdy obiektem badanym jest komputer, który musi, z takich czy innych względów, cały czas pracować (np. serwer obsługujący procesy technologiczne), bądź działania prowadzone w czasie, gdy maszyna została zdalnie przejęta przez napastnika, mające na celu jego identyfikację *in flagrante delicto* (wówczas stosuje się metody z grupy tzw. *live forensic*). W inny sposób bada się również urządzenia takie jak smartfony czy tablety, których nie da się badać bez ich włączenia.

[106] Można rozważać, czy w sytuacjach granicznych (kiedy np. istotne jest odszukanie na dysku pojedynczego pliku, co do którego wiadomo, że nie jest w żaden sposób ukryty ani zaszyfrowany) dopuszczalna byłaby praca na oryginalnym materiale dowodowym (mniejsze jest prawdopodobieństwo choćby uszkodzenia dysku w czasie pojedynczego przeszukiwania niż w czasie robienia pełnej kopii, również czasochłonność, a co za tym idzie i koszty standardowego postępowania byłyby wyższe), niemniej, jak wskazuje praktyka, posiadanie kopii bitowej dysku jest niemal zawsze wskazane (oryginalny nośnik może ulec zniszczeniu związanemu z np. niewłaściwym magazynowaniem, mogą pojawić się dodatkowe pytania odnośnie do zawartości nośnika itd.). Jak się zatem wydaje, na takie „nieformalne" postępowanie z nośnikami można sobie pozwolić wyłącznie przy okazji działań pozasądowych, a i to tylko tych mniej istotnych, czy wymagających bardzo krótkiego czasu

wości nie powinno się prowadzić analizy sprzętu komputerowego „na miejscu", ale zlecać wydanie opinii pisemnej wraz z analizą zabezpieczonego materiału dowodowego[107]. Oczywiście w sytuacji, gdy mowa jest o zawartości maszyn, które muszą pracować w trybie ciągłym, zabezpieczenie powinno obejmować wykonanie kopii w trybie *live*, a dalsze prace powinny być prowadzone na kopiach.

2.4.2 Udział biegłego informatyka w przesłuchaniu świadków i stron

Biegły może uczestniczyć w przesłuchaniu świadków i stron, oczywiście zawsze w roli narzędzia organu procesowego, a więc podczas czynności procesowych (nie ma możliwości „samodzielnego" przesłuchania świadka przez biegłego pod nieobecność organu procesowego, wręcz przeciwnie: biegły powinien się powstrzymać od prowadzenia jakichkolwiek nieformalnych rozmów z uczestnikami postępowania). Zazwyczaj pomoc biegłe-

wykonania ekspertyzy. Oczywiście zawsze (a już szczególnie w sytuacji, która wymaga pośpiechu) należy stosować blokery zapisu.

[107] Stowarzyszenie Instytut Informatyki Śledczej (http://www.siis.org.pl/najlepsze-praktyki/zabezpieczanie.html) podaje następujące dobre praktyki związane z zabezpieczaniem dowodów elektronicznych:

- ✓ „dowód powinien być zachowany w stanie z chwili zabezpieczenia, z dokładnym odnotowaniem daty i czasu. Sama czynność zabezpieczania powinna odbyć się w obecności świadków (czy też osób przybranych przy przeszukaniu);
- ✓ zabezpieczany sprzęt i nośniki powinny być prawidłowo oznakowane, opisane i ew. oplombowane. W zależności od sprawy, numery seryjne wszystkich urządzeń wchodzących w skład systemu, powinny zostać odnotowane (ze względu na możliwość ich późniejszej zamiany). W sprawach ,w których może to być konieczne, należy fotograficznie udokumentować wszystkie elementy i połączenia wchodzące w skład danego systemu;
- ✓ jedyną możliwością autentyfikacji materiału, zakładając możliwość stwierdzenia późniejszych zmian, jest wyliczenie w momencie zabezpieczania sumy kontrolnej nośnika. Możliwość ponownego wyliczenia tej samej sumy w późniejszych etapach postępowania oraz porównanie jej z sumą z zabezpieczenia pozwala na stwierdzenie, czy materiał nie został zmieniony;
- ✓ badania powinny być prowadzone wyłącznie na kopii (utworzonej na zasadzie równości z oryginałem), tak, aby nie naruszyć wartości dowodowej oryginału i umożliwić inne (innym biegłym) badania na tym samym materiale. Z tego samego powodu, badania prowadzone na oryginale, powinny być prowadzone z użyciem technik uniemożliwiających zmiany zapisów zawartych na badanym nośniku".

go jest potrzebna w trakcie fazy zadawania pytań ukierunkowanych[108], tam gdzie zachodzi potrzeba służenia organowi procesowemu wiadomościami specjalnymi. W literaturze przedmiotu[109] stosunkowo dużo miejsca poświęca się kryminalistycznej taktyce przesłuchań, w tym metodom i technice perswazji procesowej, biegły natomiast zdecydowanie powinien rozróżniać swoją rolę procesową od roli osoby prowadzącej postępowanie przygotowawcze (śledczego), czy od roli sądu prowadzącego postępowanie sądowe i nie próbować takich technik stosować w stosunku do osoby, w przesłuchaniu której uczestniczy. Jakkolwiek może się zdarzyć, że biegły będzie w stanie zaobserwować sprzeczności w zeznaniach świadków i stron (czy sprzeczności w obrębie samych tych zeznań, czy też w stosunku do treści zeznań innych osób, dokumentów znajdujących się w aktach sprawy, czy wreszcie – nieprawdziwość treści zeznań z wiadomościami specjalnymi z dziedziny, dla której biegły jest ustanowiony) i informacje o takich sytuacjach powinien przekazać organowi procesowemu, to cały czas powinien pamiętać o roli tego organu, który prowadzi przesłuchanie i o swojej roli narzędzia tegoż organu.

W opiniowaniu informatycznym uwidacznia się dość nietypowy problem związany z przesłuchaniem świadków dysponujących wiadomościami specjalnymi. We współczesnym KPK (art. 196 § 1) oraz Kodeksie postępowania administracyjnego (dalej KPA) – art. 84 § 2, nie jest możliwe łączenie roli biegłego oraz świadka, zgodnie natomiast z art. 281 KPC bycie świadkiem może być powodem żądania przez stronę wyłączenia biegłego i – zgodnie z orzecznictwem – fakt bycia świadkiem z reguły uniemożliwia pełnienie

[108] Przesłuchanie zazwyczaj składa się ze wstępnej swobodnej wypowiedzi przesłuchiwanego (w odpowiedzi na pytania ogólne np. „co może Pani/Pan powiedzieć w tej sprawie") oraz części zawierającej pytania szczegółowe organu prowadzącego przesłuchanie (zwanej też fazą pytań ukierunkowanych). Zob. np.: M. Maciejski: *Psychologiczna analiza sposobów przesłuchania świadków i reguł oceny ich zeznań w praktyce sędziowskiej a stopień przypisywanej im wiarygodności*, Katowice 2009, praca doktorska, maszynopis, http://www.sbc.org.pl/Content/19427/doktorat3009.pdf, s. 247 i nast.

[109] Zob. np.: J.P. Kufel: *Taktyka przesłuchania świadka*, „Edukacja Prawnicza" z 13 października 2009 r., http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualnosc/art/taktyka-przesluchania-swiadka.html; M. Maciejski: *Psychologiczna*…, op. cit.; E. Gruza: *Ocena wiarygodności zeznań świadków w procesie karnym*. *Problematyka kryminalistyczna*, Zakamycze, Kraków 2003.

funkcji biegłego[110]. W przypadku części zagadnień informatycznych świadkami zdarzeń są osoby posiadające nie tylko wiedzę wysoce specjalizowaną, ale również unikatowe informacje dotyczące zasad działania dedykowanego oprogramowania własnego autorstwa[111]. W ten sposób świadek oczywiście najbardziej „biegły" (w sensie potocznym) w kwestiach dotyczących programu własnego autorstwa nie może być biegłym (w sensie prawa), z uwagi na przytoczone wyżej zakazy. Pojawiają się tu co najmniej dwie sytuacje wysoce niekomfortowe:

1) dialog świadka z biegłym może pozostać zupełnie niezrozumiały dla organu procesowego i pozostałych uczestników postępowania;
2) przekazanie biegłemu informacji dotyczących funkcjonowania konfiguracji, sposobu użytkowania) znanego świadkowi oprogramowania, czy systemu informatycznego może być długotrwałe i wymagać raczej demonstracji niż komunikacji werbalnej.

Wydaje się, że można dać tutaj następujące wskazówki postępowania:

- ✓ należy raczej dążyć do rejestracji zeznań świadka tego rodzaju w postaci nagrania, niż do ich tradycyjnego protokołowania, jest bowiem wysoce prawdopodobne, że protokolant będzie miał trudność ze zrozumieniem wypowiedzi świadka, a konieczność dyktowania ich do protokołu wybitnie zaburzy wypowiedź i utrudni przekazanie rzeczowych informacji;
- ✓ po uzyskaniu interesujących informacji od świadka, biegły może spróbować sformułować je w sposób możliwie zrozumiały dla osób nieposiadających wiadomości specjalnych i uzyskać od świadka potwierdzenie, że sformułowanie to jest prawidłowe (przy czym oczywiście należy pamiętać o obowiązujących zasadach zadawania

[110] Zob. wyrok Sądu Najwyższego z 8 listopada 1976 r. (I CR 374/76): „Osoba, która z racji posiadanych wiadomości specjalnych ma spostrzeżenia niedostępne dla innych osób (np. lekarz leczący chorego), powinna z reguły być słuchana w charakterze świadka, a funkcję biegłego należy powierzyć innej osobie, która z faktami istotnymi dla rozstrzygnięcia sprawy poprzednio się nie zetknęła". Por. np. G. Kopczyński: *Konfrontacja biegłych w polskim procesie karnym*, Wolters Kluwer business, Warszawa 2008, s. 101 i nast.

[111] Sytuacja taka ma miejsce szczególnie w przypadku nietypowych programów, pisanych na zamówienie („pod klucz") przez któregoś z uczestników postępowania, które to programy świadek pisał i wdrażał, zapoznając się przy okazji z okolicznościami istotnymi później w sprawie sądowej.

pytań, w szczególności o zakazie sugerowania osobie przesłuchiwanej treści odpowiedzi[112] – art. 171 § 4 KPK), ewentualnie poprosić osobę przesłuchiwaną o sformułowanie odpowiedzi w sposób możliwie zrozumiały dla uczestników postępowania;

- ✓ jeśli wskazane byłoby przekazanie przez świadka informacji przez demonstrację (np. sposobu działania systemu), należy rozważyć przeprowadzenie eksperymentu procesowego[113] przy wykorzystaniu kopii badanego systemu (uprzednio uzyskanej, oczywiście również w przewidzianym przepisami trybie). Należy przy tym pamiętać, że KPK w art. 212 pozwala na łączenie eksperymentu procesowego z innymi czynnościami dowodowymi (*explicite* wymienione jest przesłuchanie), podczas gdy alternatywne organizowanie wyjazdowego posiedzenia sądu „przy serwerze" połączonego z przesłuchaniem świadka i oględzinami oryginalnego systemu przeprowadzonymi z udziałem biegłego może być co najmniej wątpliwe, a na pewno stosunkowo niebezpieczne, jeśli nie ze względów prawnych, to z punktu widzenia bezpieczeństwa danych i systemów informatycznych.

[112] Por. np. M. Maciejski: *Psychologiczna*…, op. cit., s. 263–264. Wydaje się, że w zakresie doprecyzowania używanej terminologii, czy wyrażenia w sposób czytelny informacji przekazanej przez świadka, lepsze jest mimo wszystko zapytanie go o to, czy to, co zeznał da się wyrazić we wskazany przez biegłego sposób (np. „czy dobrze zrozumiałem, że świadek zaobserwował wyświetlenie komunikatu o błędzie na monitorze?") niż próba tłumaczenia (już po złożeniu zeznań, pod nieobecność świadka) sądowi, co biegły zrozumiał z tego, co świadek powiedział (np. „świadek powiedział, że wyświetlił się błąd, więc zapewne zobaczył komunikat o błędzie wyświetlony na monitorze").

[113] Eksperyment procesowy jest środkiem dowodowym opisanym w art. 211 KPK. KPC ani KPA nie zawierają uregulowań dotyczących eksperymentu, choć – jak słusznie zauważa np. Małgorzata Żołna – wobec otwartego charakteru katalogu środków dowodowych można spodziewać się, że może on znaleźć zastosowanie również w postępowaniu cywilnym i administracyjnym (M. Żołna: *Eksperyment procesowo-kryminalistyczny. Istota i dowodowa rola*, Difin, Warszawa 2011, s. 24 i nast.).

2.4.3 Udział biegłego informatyka w eksperymencie procesowym i w oględzinach

Eksperyment (łac. *experimentum* – próba) procesowy jest czynnością dowodową[114] organu procesowego o charakterze w zasadzie niepowtarzalnym, jakkolwiek w przypadku jego niepowodzenia, to jest uznania jego przebiegu lub wyniku za nieprawidłowy przez organ procesowy (którego ocenie eksperyment, na zasadzie swobodnej oceny dowodów podlega), możliwe jest jego powtórzenie.

Należy odróżnić eksperymenty, które może prowadzić biegły w ramach badań koniecznych do wydania opinii (eksperyment rzeczoznawczy) od eksperymentu procesowego, będącego czynnością organu procesowego[115]. W tym pierwszym przypadku eksperyment jest związany z wyborem odpowiedniej metody badawczej przez biegłego (a więc jest skutkiem jego decyzji mieszczącej się w ramach autonomii biegłego) i jest częścią procesu przygotowania przez biegłego ekspertyzy, w tym drugim – jest to czynność procesowa prowadzona przez organ procesowy, zgodnie z zasadami postępowania określonymi przepisami prawa (a więc np. zasadą jawności czy bezpośredniości).

Na marginesie można zauważyć, że wymogi prawa i zdrowy rozsądek nakładają na biegłego pewne ograniczenia metodologiczne również w zakresie sposobu prowadzenia eksperymentów rzeczoznawczych: w szczególności w ramach ewentualnych eksperymentów rzeczoznawczych biegły nie powinien usiłować wykonywać czynności zastrzeżonych dla organu procesowego (a więc np. próbować przesłuchiwać świadków i strony, dokonywać oględzin, zabezpieczać dowody rzeczowe itd.)[116].

---

[114] Zob. np.: M. Żołna: *Eksperyment*…, op. cit., s. 155 i nast.; J. Wojtasik: *Eksperyment procesowo-kryminalistyczny*, http://www.zielona-gora.po.gov.pl/index.php?id=36&ida=2869.

[115] Zob. wyrok Sądu Najwyższego z 23 czerwca 1988 r. (I KR 174/88): „Główną cechą odróżniającą eksperyment procesowy od eksperymentu rzeczoznawczego jest to, że eksperyment przeprowadzony w postępowaniu dowodowym przez sąd i inne organy procesowe jest *sensu stricto* czynnością procesową, natomiast eksperyment rzeczoznawczy przymiotu takiego nie ma; jest częścią składową opinii biegłego. Druga cecha odróżniająca obie te czynności dotyczy podmiotów dokonujących badań. Eksperyment rzeczoznawczy jest przeprowadzany przez biegłych różnych specjalności, natomiast eksperyment procesowy jest czynnością organu procesowego prowadzącego postępowanie karne".

[116] Artykuł V. Kwiatkowskiej-Wójcikiewicz*: Glosa do wyroku Sądu Najwyższego z 3 października 2006 r., (IV KK 209/06)*, „Prokuratura i Prawo" Nr 9/2009, s. 148–154; zawiera glossę (aprobu-

Eksperyment procesowy ma na celu sprawdzenie hipotezy dotyczącej faktu istotnego dla rozstrzygnięcia określonej kwestii mającej znaczenie dla przebiegu postępowania[117].

Artykuł 211 KPK rozróżnia dwa rodzaje eksperymentu[118]: doświadczenie oraz odtworzenie przebiegu stanowiących przedmiot rozpoznania zdarzeń lub ich fragmentów.

> ***Art. 211.***
>
> *W celu sprawdzenia okoliczności mających istotne znaczenie dla sprawy można przeprowadzić, w drodze eksperymentu procesowego, doświadczenie lub odtworzenie przebiegu stanowiących przedmiot rozpoznania zdarzeń lub ich fragmentów.*

W zakresie zainteresowania biegłego informatyka leżeć będą raczej nie rekonstrukcje zdarzeń, ale doświadczenia, które mogą prowadzić do falsyfikacji (ewentualnie potwierdzenia) stawianych hipotez.

Nie zagłębiając się zbytnio w kwestie formalno-metodologiczne dotyczące eksperymentów, należy wspomnieć o dwóch, nie zawsze dobrze rozumianych, uwarunkowaniach dotyczących ich prowadzenia:

- ✓ w literaturze[119] można znaleźć wymóg poczynienia przez badacza założenia wstępnej hipotezy badawczej, która ma zostać

jącą) do wyroku Sądu Najwyższego, w której autorka omawia sytuację, do jakiej doszło w wyniku przeprowadzenia przez biegłego takich quasi-oględzin (wizji lokalnej):
„W omawianej sprawie biegły nie tylko dokonał wizji lokalnej i przeprowadził eksperyment, ale także przesłuchiwał w jego trakcie oskarżoną, pokrzywdzoną i świadka. Był tak »sumienny«, że sporządził nawet protokół z wizji lokalnej i eksperymentu procesowego, w których zamieścił »zeznania przesłuchiwanych«. Informacje uzyskane tym sposobem przez biegłego stały się podstawą jego opinii, a nie powinny. Taka opinia powinna być zdyskredytowana przez sąd, a niestety stała się podstawą wydanych wyroków w obu instancjach. Mało tego, sąd wyższej instancji, próbował konwalidować opinię biegłego, utrzymując, że biegły przeprowadził eksperyment rzeczoznawczy. Z takim stwierdzeniem słusznie nie zgodził się Sąd Najwyższy, stwierdzając w uzasadnieniu, że »eksperyment rzeczoznawczy nie legalizuje ani przesłuchania przez niego (biegłego – przyp. autorki) uczestników postępowania, ani tym bardziej wykorzystania ich oświadczeń i to również przez Sąd odwoławczy«".

[117] Zob. A. Gaberle: *Dowody w sądowym procesie karnym*, Wolters Kluwer, Warszawa 2007, s. 220.

[118] W literaturze przedmiotu (np. ibid., s. 221) zwane czasem, niezbyt trafnie, formami eksperymentu.

[119] Zob. np.: A. Malasińska-Nagórny: *Eksperyment prowadzony na podstawie art. 211 KPK a eksperyment rzeczoznawczy*, „Kwartalnik procesowo-kryminalistyczny" Nr 1–2 (10–11)/2012,

potwierdzona lub sfalsyfikowana w wyniku przebiegu eksperymentu. Oczywiście nie jest konieczne, aby każdy problem badawczy przedstawiać w postaci pytania alternatywnego (czy prawdziwe jest zdanie, będące hipotezą badawczą). Możliwe i dopuszczalne są badania mające na celu uzyskanie odpowiedzi na pytania inne, niż pytania o prawdziwość założonej hipotezy. Na przykład można przeprowadzić badanie odpowiadające na pytanie, ile wynosi średni wzrost w badanej grupie studentów, nie formułując żadnych hipotez; wystarczy dokonać pomiaru wzrostu każdego ze studentów i obliczyć wartość średnią. Inaczej natomiast będzie wyglądała kwestia, gdy trzeba będzie z badania próby wyciągać wnioski o parametrach charakteryzujących całą populację. Podówczas rzeczywiście trzeba skorzystać z metod statystycznej weryfikacji hipotez, aby móc odpowiednio zaplanować sposób przeprowadzenia badania (w tym dobór odpowiedniej próby badawczej) i uogólnić otrzymane wnioski;

- ✓ symulacja obliczeniowa[120] nie jest – *sensu stricto* – z metodologicznego punktu widzenia badaniem eksperymentalnym[121], ale – jeśli można w ogóle w ten sposób klasyfikować metody badań – szczególnym rodzajem badania teoretycznego, podobnie jak jest nim np. obliczanie na papierze, czy przy użyciu kalkulatora wartości funkcji matematycznej dla różnych wartości argumentów. Różnica między tymi sytuacjami polega przecież jedynie na szybkości działania użytego narzędzia. To, że współczesna technika kom-

http://pila.szkolapolicji.gov.pl/joomla/images/Zamowienia/Kwartalnik/Nr10-11/02eksperyment.pdf.

[120] W literaturze przedmiotu używa się powszechnie pojęć „symulacja komputerowa" (ang. *a computer simulation*) i „modelowanie komputerowe" (ang. *a computer modeling*, *a computational modeling*). Są to oczywiście pojęcia poprawne (słowo *computer* pochodzi od *compute* – obliczać). Biorąc jednak pod uwagę, że w informatyce mowa może być również o symulacji (generowaniu, preparowaniu, odtwarzaniu) np. ruchu sieciowego, co odbywa się przy wykorzystaniu urządzeń techniki komputerowej należy dla czytelności rozróżnić „symulację obliczeniową", w której komputer służy do prowadzenia obliczeń od „symulacji komputerowej", lub szerzej, np. jako generator pakietów, które następnie używane są do testowania wydajności urządzeń sieciowych, czy ich zgodności z odpowiednimi protokołami.

[121] Por. np. J. Wojtasik: *Eksperyment*…, op. cit.

puterowa umożliwia atrakcyjne wizualnie (czy nawet multimedialnie) prezentowanie otrzymanych wyników, a także oferuje często niewyobrażalną moc obliczeniową, pozwalającą na korzystanie z niezwykle złożonych modeli matematycznych, rzeczywiście zbliża przebieg współczesnej symulacji do klasycznego eksperymentu, w którym badacz dokonuje modyfikacji w obrębie przedmiotu i okoliczności badania dla ustalenia związków pomiędzy poszczególnymi elementami. Stąd też tego rodzaju operacje na modelach nazywa się czasem „badaniami paraempirycznymi" czy „eksperymentami zastępczymi".

Odnośnie do oględzin to, jak wspomniano wyżej, są one również czynnością organu procesowego[122], wykonywaną zawsze przez organ procesowy (a więc w postępowaniu sądowym przez sąd) w razie konieczności z udziałem biegłego, nigdy natomiast przez samego biegłego. Niestety, w wyniku niechlujstwa językowego[123], stosunkowo często oględzinami nazywa się czynności badawcze, prowadzone przez biegłych w ramach przygotowania opinii[124].

[122] Wypowiedział się na ten temat np. Sąd Najwyższy: „Oględziny (art. 207 § 1 KPK) i eksperyment (art. 211 KPK) to czynności procesowe, przeprowadzane wyłącznie przez organ procesowy, który może wezwać do nich biegłego (art. 198 § 1 KPK) lub specjalistę (art. 205 § 1 KPK)". Zob. wyrok Sądu Najwyższego z 3 października 2006 r. (IV KK 209/06, OSNKW Nr 12/2006, poz. 114). Zob. też np. M. Szmit: *Z całą…*, op. cit.; J. Jerzewska: *Od oględzin do opinii biegłego. Poradnik dla prowadzących postępowanie karne*, Dom Wydawniczy ABC, Warszawa 2005 (wydanie 2). Tak samo oględziny jako czynność sądu są opisane w art. 292 KPC (Sąd może zarządzić oględziny bez udziału lub z udziałem biegłych, a stosownie do okoliczności – również w połączeniu z przesłuchaniem świadków). Należy mieć to na względzie również w przypadku żądania zabezpieczenia dowodu w procesie cywilnym w trybie art. 310 KPC. Czasami rozróżnia się oględziny karno-procesowe, prowadzone w ramach postępowania przygotowawczego (oględziny dochodzeniowe lub oględziny śledcze) oraz oględziny sądowe, czyli prowadzone przez sąd w toku postępowania dowodowego. Zob. N. Tuła: *Oględziny i ich rodzaje*, „Edukacja Prawnicza" z 17 września 2010 r., http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualność/art/ogledziny-i-ich-rodzaje.html.

[123] Zob. np.: A. Słodki: *W opinii biegłego – niewykonanie umowy w terminie*, „Nieruchomości" Nr 2(30)/2001; postanowienie Sądu Apelacyjnego w Krakowie z 13 lutego 2012 r. (ACz 164/12).

[124] Szczególnie dotyczy to czynności prowadzonych przez geodetów, rzeczoznawców samochodowych i rzeczoznawców majątkowych, które wymagają zapoznania się ze stanem nieruchomości (bądź uszkodzonego pojazdu), co odbywa się często w drodze wizyty rzeczo-

W przypadku biegłych informatyków tego rodzaju zlecenia wykonania „oględzin przez biegłego" zdarzają się stosunkowo często[125] i jedyną właściwą – choć wysoce stresującą dla biegłego – odpowiedzią jest w takim przypadku odmowa wykonania polecenia sądu. Pomijając zresztą nawet aspekty prawne, tego rodzaju czynności nie prowadzą zazwyczaj do zamierzonych skutków, z szeregu powodów:

- ✓ biegły nie ma kompetencji decyzyjnych np. odnośnie do zabezpieczenia ujawnionych śladów dowodowych, które w trakcie takiej „wizji" mógłby odnaleźć;
- ✓ poza salą sądową, a dokładniej poza czasem trwania czynności procesowych (samodzielne wyprawy biegłego „po śladach" takimi nie są), biegły nie podlega żadnej szczególnej ochronie prawnej, a więc wszelkie skutki nieprzewidywanych zdarzeń obciążają biegłego;
- ✓ wywiady swobodne ze świadkami nie są ani metodą badawczą informatyki, ani dowodami w sprawie;
- ✓ może się więc okazać niemożliwe nawet ustalenie, o jaki komputer czy urządzenie chodzi, czy uzyskanie dostępu do niego;
- ✓ polecenie, które sąd wyda biegłemu, nie wiąże w żaden sposób posiadacza urządzenia, który może, a często nawet powinien, odmówić osobie postronnej ingerencji w swój system informatyczny.

Jedyną możliwością (poza uzupełnieniem dowodów przez prokuraturę, jeżeli mowa o postępowaniu karnym) jest przeprowadzenie oględzin przez sąd z udziałem biegłego. Bywa to działanie czasochłonne i trudne w realizacji (może wymagać zorganizowania wyjazdowego posiedzenia sądu), niemniej jest to jedyny sposób, aby dokonać oględzin zgodnie z prawem.

Jak wspomniano wyżej, nie ma również możliwości konwalidacji takich „oględzin biegłego" poprzez uznanie ich za eksperyment procesowy.

Od strony technicznej do oględzin można odnieść wszystkie uwagi, jakie odnoszą się do zabezpieczenia procesowego dowodów elektronicznych

znawcy na terenie nieruchomości, bądź w miejscu, w którym znajduje się pojazd. Tego rodzaju czynności są jednak czynnościami badawczymi eksperta, a nie oględzinami, które zawsze są czynnością organu procesowego.

[125] Szczególnie gdy mowa o systemach komputerowych znajdujących się w siedzibach różnych organizacji.

(a więc postulat należytej dbałości o integralność badanego systemu i danych, konieczność odpowiedniego przygotowania do przeprowadzenia czynności, w tym zaplanowania prowadzonych działań, konieczność rejestracji bądź protokołowania przebiegu czynności itd.).

Przy okazji omawiania zadań biegłego jako narzędzia sądu warto wspomnieć o sytuacji, niemającej *de facto* umocowania w przepisach obowiązującego prawa: wykorzystania biegłego w roli konsultanta składu orzekającego. Zdarza się ona często jeszcze przed wydaniem postanowienia o powołaniu: sędzia (lub prokurator) potrzebuje uzyskać informację, bądź to o samych technicznych czy naukowych aspektach zagadnienia pełniącego istotną rolę w postępowaniu, bądź wręcz potrzebuje pomocy w prawidłowym sformułowaniu pytań do biegłego, które mają być zawarte w postanowieniu o jego powołaniu. O ile w postępowaniu przygotowawczym kontakt prokuratora z biegłym zaangażowanym w postępowanie nie budzi wątpliwości, o tyle w postępowaniu sądowym wszystkie kontakty biegłego z sądem (a w zasadzie ze składem orzekającym) powinny być jawne i udokumentowane z uwagi na zasadę jawności postępowania. Z drugiej strony źle postawione pytania, czy niewłaściwe użycie terminów fachowych (nie mówiąc już np. o braku orientacji sędziego, co do natury przedmiotu sporu) prowadzi w najlepszym razie do niepotrzebnego przedłużania postępowania. W praktyce tego rodzaju ustalenia prowadzone są stosunkowo często przed powołaniem biegłego[126],

[126] W zasadzie można je podówczas zakwalifikować jako nieformalne konsultacje, udzielone prywatnie, przez osobę niepełniącą przecież w tym momencie roli biegłego innej osobie prywatnej, która zawodowo jest funkcjonariuszem wymiaru sprawiedliwości, w czym trudno dopatrywać się jakiegokolwiek przekroczenia zasad prawa czy etyki. Być może należałoby rozważyć celowość wprowadzenia do przepisów procesowych usankcjonowania tego rodzaju „opinii konsultacyjnych". Jak piszą autorzy w poświęconym biegłym raporcie Helsińskiej Fundacji Praw Człowieka: „Za pożądaną praktykę należy uznać konsultowanie z biegłymi pytań, które mają znaleźć się w postanowieniu o zasięgnięciu opinii. Pozwala to znacznie skrócić czas, w którym ostateczna opinia trafia w ręce decydenta procesowego, a także chroni, przed pojawieniem się ewentualnych zarzutów pod adresem sporządzonej opinii. Powoływanie ekspertów bez uwzględnienia wspomnianych okoliczności, prowadzi natomiast najczęściej do mnożenia opinii. Konieczne staje się wydawanie postanowień uzupełniających pytania zadane uprzednio biegłemu, zdarzają się opinie niejasne, niepełne lub wewnętrznie sprzeczne" (B. Grabowska, A. Pietryka, M. Wolny, A. Bodnar: *Raport HFPC: Biegli sądowi w Polsce*, http://www.hfhr.pl/wp-content/uploads/2014/04/HFPC_PRB_biegli-sa%CC%A8dowi_w_polsce.pdf, s. 37).

natomiast nie powinny mieć miejsca już po jego powołaniu, kiedy to wszelkie wątpliwości należy wyjaśniać w sposób procesowy.

3 Metodyka ekspertyzy – uwagi ogólne

Rola źródła dowodowego – wydawanie opinii sądowej – jest, zgodnie z tym co napisano powyżej, zasadniczą i najczęściej spotykaną rolą biegłego sądowego.

W postępowaniu karnym, celem zarówno oskarżyciela, jak i sądu (którego narzędziem jest biegły), jest ustalenie prawdy materialnej[127], co ułatwia zadanie biegłemu o tyle, że może on formułować np. postulaty odnośnie do tego, co powinno zostać zbadane.

W postępowaniu cywilnym również obowiązuje zasada prawdy materialnej, nie ma ona jednak charakteru bezwzględnego, ustawodawca bowiem wielokrotnie ogranicza ją, pozwalając w wielu przypadkach na poprzestanie na „prawdzie" formalnej. Szczególnie ważną, z punktu widzenia biegłego, cechą postępowania procesowego w sprawach cywilnych jest większe, niż w procesie karnym, znaczenie zasady kontradyktoryjności. Konsekwencją tego stanu rzeczy może być ograniczenie aktywności biegłego. Z uwagi na różnice między rygorami postępowań: karnego i cywilnego, osobny rozdział (5) poświęcono opiniowaniu w tych ostatnich.

Decyzja o zasięgnięciu opinii biegłego jest podejmowana przez organ procesowy w przypadku, w którym dla rozpoznania sprawy wymagane jest posiadanie wiadomości specjalnych, przy czym w przypadku postępowania karnego i postępowania o wykroczenia, powołanie biegłego w sytuacji, w której stwierdzenie okoliczności, mających istotne znacznie dla rozstrzygnięcia sprawy, wymaga wiadomości specjalnych, jest obligatoryjne na mocy

[127] Stąd też z najwyższym uznaniem należy ocenić pracę biegłych w zdarzających się czasami przypadkach, w których biegły, pomimo zgodnej postawy oskarżyciela wnoszącego akt oskarżenia i oskarżonego, przyznającego się do winy, jest w stanie np. sfalsyfikować opis okoliczności zdarzenia i wykazać niewinność oskarżonego. Zob. np.: R. Zachorski: *Metodyka…*, op. cit., s. 118 i nast.

przepisów KPK, w sprawach cywilnych natomiast w orzecznictwie panuje zgoda, że powołanie biegłego w takiej sytuacji również jest obowiązkiem sądu[128].

3.1 Postanowienie o zasięgnięciu opinii

Proces opiniowania sądowego formalnie rozpoczyna się od wydania przez organ procesowy (sąd bądź organ prowadzący postępowanie przygoto-

[128] Odpowiednie przepisy stanowią jak następuje:
Art. 193 § 1 KPK: „Jeżeli stwierdzenie okoliczności mających istotne znacznie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych, zasięga się opinii biegłego albo biegłych". Art. 278 § 1 KPC: „W wypadkach wymagających wiadomości specjalnych sąd po wysłuchaniu wniosków stron co do liczby biegłych i ich wyboru może wezwać jednego lub kilku biegłych w celu zasięgnięcia ich opinii". Art. 84 § 1 KPA: „Gdy w sprawie wymagane są wiadomości specjalne, organ administracji państwowej może zwrócić się do biegłego lub biegłych o wydanie opinii". Sformułowanie „może zwrócić się" wydaje się sugerować pozostawienie organowi procesowemu swobody w ocenie, czy konieczne jest zasięgnięcie opinii biegłego, natomiast sformułowanie „zasięga się" – sugeruje, że intencją ustawodawcy nie było pozostawienie organowi procesowemu takiej swobody (por. np. A. Kegel, Z. Kegel: *Przepisy...*, op. cit., s. 16 i nast.), orzecznictwo Sądu Najwyższego wskazuje jednak, że również w sprawach cywilnych powołanie biegłych jest obligatoryjne (zarówno jeśli idzie o wnioskowanie przez stronę o przeprowadzenie dowodu z opinii biegłego, jak i o powołanie biegłego z inicjatywy sądu, o ile sąd dojdzie do przekonania, że okoliczność mająca istotne znaczenie dla prawidłowego rozstrzygnięcia sprawy może zostać wyjaśniona tylko w wyniku wykorzystania wiedzy osób posiadających wiadomości specjalne:

- ✓ w wyroku z 3 lutego 2010 r. [II PK 192/09] Sąd Najwyższy stwierdził: „W orzecznictwie Sądu Najwyższego przyjmuje się, że mimo fakultatywnej formuły przytoczonego przepisu, sąd musi zwrócić się do biegłego, jeśli dojdzie do przekonania, że okoliczność mająca istotne znaczenie dla prawidłowego rozstrzygnięcia sprawy może zostać wyjaśniona tylko w wyniku wykorzystania wiedzy osób mających specjalne wiadomości. W takim przypadku dowód z opinii biegłego z uwagi na składnik wiadomości specjalnych jest dowodem tego rodzaju, że nie może być zastąpiony inną czynnością dowodową ani wnioskowaniem na podstawie innych ustalonych faktów";
- ✓ w wyroku z 19 grudnia 2012 r. [II CNP 41/12] Sąd Najwyższy stwierdził: „Pominięcie dowodu zgłaszanego przez stronę jest bowiem dopuszczalne wtedy, gdy okoliczności sporne, na które dowód powołano, zostały dostatecznie wyjaśnione zgodnie ze stanowiskiem strony powołującej dowód (wyroki Sądu Najwyższego z 12 stycznia 2005 r., I CK 451/04, niepubl.; z 5 lutego 2009 r., II UK 176/08, niepubl. i z 13 grudnia 2010 r., III SK 16/10, niepubl.)".

wawcze w sprawach karnych) postanowienia o zasięgnięciu opinii biegłego[129]. Postanowienie o zasięgnięciu opinii biegłego w postępowaniu karnym[130] powinno zawierać elementy, o których mowa w art. 94 KPK, tj.:

1) oznaczenie organu oraz osoby lub osób, wydających postanowienie;

2) datę wydania postanowienia;

3) wskazanie sprawy oraz kwestii, której postanowienie dotyczy;

4) rozstrzygnięcie z podaniem podstawy prawnej;

5) uzasadnienie, chyba że ustawa zwalnia od tego wymagania

oraz elementy, o których mowa w art. 194 KPK, tj.:

1) imię nazwisko i specjalność biegłego lub biegłych, a w wypadku opinii instytucji, w razie potrzeby, specjalność i kwalifikacje osób, które powinny wziąć udział w przeprowadzeniu ekspertyzy;

2) przedmiot i zakres ekspertyzy ze sformułowaniem, w miarę potrzeby, pytań szczegółowych;

3) termin dostarczenia opinii.

Warto zwrócić uwagę, że KPK posługuje się zamiennie pojęciem opinii i ekspertyzy (art. 194 ust. 1 i ust. 2). Część autorów[131] zwraca uwagę, że być może trafniej byłoby nazywać „opinią" tę część ekspertyzy, w której biegły zamieszcza wnioski (te bowiem są wynikiem indywidualnego procesu intelektualnego konkretnego biegłego), natomiast w szerokim znaczeniu posługiwać się pojęciem „ekspertyza", niemniej obecnie używa się na oznaczenie środka dowodowego będącego efektem pracy biegłego pojęcia „opinia".

[129] Nie są dopuszczalne inne formy zlecenia przez organ procesowy biegłemu wykonania opinii (np. zarządzenie). W przypadkach niecierpiących zwłoki powołanie biegłego może nastąpić w innej formie niż pisemne postanowienie, choć musi ono w dalszym ciągu postępowania być potwierdzone we właściwej formie procesowej. Zob. K. Eichstaedt, P. Gałecki, A. Depko: *Metodyka*…, op. cit., s. 105 i nast.

[130] KPC i KPA, mimo że zawierają w sobie przepisy o biegłych, nie precyzują tak szczegółowo wymogów odnośnie do postanowienia o ich powołaniu.

[131] Zob. np.: J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 41; G. Kopczyński: *Konfrontacja*…, op. cit., s. 67 i nast.

3.2 Określenie zakresu i przedmiotu opinii

Z punktu widzenia biegłego najważniejszą częścią postanowienia jest określenie przedmiotu i zakresu ekspertyzy, które dane są sformułowanymi w niej pytaniami i poleceniami[132]. Zakres opinii zakreślony jest pytaniami postawionymi przez organ procesowy (sąd bądź organ prowadzący postępowanie przygotowawcze w sprawach karnych), bądź opisem czynności, jakie biegły powinien wykonać. Badania prowadzone przez biegłego nie mogą wykraczać poza zakres opinii, zaś wnioski (konkluzja) opinii powinna, w miarę możliwości, odpowiadać na postawione pytania. Zarówno w swoich działaniach, jak i w wypowiedziach, biegły nie powinien wykraczać poza zakres opinii. Od tej zasady mogą zachodzić wyjątki (np. jeśli biegły na skutek badania materiału dowodowego uzyskał wiedzę o popełnionym przestępstwie: jego obowiązkiem jest wówczas zawiadomić organ procesowy[133]).

W postanowieniu o zasięgnięciu opinii biegłego organ procesowy wskazuje przedmiot opinii, a więc również przedmiot badania[134], w tym fakt

[132] Por. np. W. Przybyło: *Postanowienie o dopuszczeniu dowodu z opinii biegłego w teorii i praktyce*, „Edukacja Prawnicza" z 13 października 2009 r., http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualnosc/art/postanowienie-o-dopuszczeniu-dowodu-z-opinii-bieglego-w-teorii-i-praktyce; T. Tomaszewski: *Postanowienia o powołaniu biegłego w teorii i praktyce*, „Problemy Kryminalistyki" Nr 163/1984, s. 66–69.

[133] W przypadku badania tzw. dowodów elektronicznych, w szczególności nośników danych może to być np. znalezienie na nich treści, które nie powinny się były tam znaleźć (np. informacji tajnych na prywatnym komputerze użytkownika, który nie powinien do takiej informacji mieć dostępu). Warto pamiętać, że biegły nie jest kompetentny do rozstrzygania o tym, czy rzeczywiście przestępstwo miało miejsce: jest to zadanie organu procesowego (w szczególnym przypadku, jeśli sąd podzieli podejrzenia biegłego, to sąd powiadomi prokuraturę). Oczywiście wszelkie takie informacje od biegłego do sądu powinny mieć formę pisemną. Warto też pamiętać, że dowody popełnienia przestępstwa mogą zostać znalezione również przy okazji opiniowania w sprawach cywilnych czy w postępowaniu administracyjnym. Nie zmienia to sytuacji: biegły – będąc niesamodzielnym organem wymiaru sprawiedliwości – ma obowiązek powiadomienia organu procesowego o powziętym podejrzeniu.

[134] Specyficznym rodzajem opinii są opinie abstrakcyjne, to jest opinie niewymagające badania materiału dowodowego. Tego rodzaju opinie służą zazwyczaj wyjaśnieniu organowi procesowemu istniejącego stanu nauki bądź praktyki w opiniowanym zakresie, w tym np. stosowanych rozwiązań technicznych czy funkcjonujących w danej dziedzinie technologii. W ramach tego rodzaju opinii biegły nie prowadzi badań (wyjąwszy ewentualne badania literaturowe).

umożliwienia biegłemu dostępu do materiału dowodowego (akt sprawy[135] oraz dowodów rzeczowych).

[135] Artykuł 198 § 1 KPK „W miarę potrzeby udostępnia się biegłemu akta sprawy w zakresie niezbędnym do wydania opinii i wzywa się go do udziału w przeprowadzeniu dowodów". Artykuł 284 KPC: „Sąd może zarządzić okazanie biegłemu akt sprawy i przedmiotu oględzin oraz zarządzić aby brał udział w postępowaniu dowodowym".
Kwestia dostępu biegłego do akt sprawy podnoszona była wielokrotnie w piśmiennictwie (zob. np.: J. Wojtasik: *Akta sprawy jako materiał badawczy w ekspertyzie*, http://www.zielonagora.po.gov.pl/index.php?id=36&ida=8265). Zasadniczo za udostępnieniem biegłemu dostępu do całości akt sprawy przemawiają następujące przesłanki:

- ✓ biegły może zapoznać się z całością informacji dostępnej organowi procesowemu, którego jest narzędziem, może w tym materiale znaleźć informacje, które w świetle wiadomości specjalnych, pozwolą mu odpowiedzieć na postawione pytania, a które mogłyby być pominięte, gdyby organ procesowy ograniczył biegłemu dostęp do akt sprawy (organ procesowy może nie ocenić właściwie znaczenia jakiegoś fragmentu materiału dowodowego, nie posiada bowiem wiadomości specjalnych, które ma biegły);
- ✓ źle dokonana selekcja materiału dowodowego może stać się przyczyną wyciągnięcia wniosków o niewłaściwym stopniu kategoryczności, bądź wniosków błędnych, a nawet stać się podstawą zarzutu, że opinia nie uwzględnia wszystkich istotnych okoliczności wynikających z akt sprawy (por. np. K. Eichstaedt, P. Gałecki, A. Depko: *Metodyka…*, op. cit., s. 120).

Argumentami przemawiającymi za daleko idącą selekcją akt udostępnianych biegłemu są natomiast:

- ✓ ekonomia postępowania: konieczność zapoznania się biegłego z aktami liczącymi czasem przecież kilkadziesiąt, czy kilkaset tomów, implikuje wydłużenie czasu i kosztów opiniowania, stosunkowo często natomiast treść akt sprawy nie ma wpływu na jakość wydanej opinii. Jak pisze słusznie J. Wojtasik, przykładem takich sytuacji mogą być klasyczne techniczne ekspertyzy identyfikacyjne w sprawach dowodowo niepowikłanych. „Poza postanowieniem i dobrze oznaczonym i opakowanym materiałem dowodowym oraz porównawczym, nie ma w wielu przypadkach potrzeby przekazywania do laboratorium kryminalistycznego innych materiałów procesowych" (J. Wojtasik: *Akta…*, op. cit.);
- ✓ trudność w konstruowaniu opinii opierającej się na zeznaniach świadków, w szczególności jeśli świadkowie ci zostali lub mogą zostać w przyszłości oskarżeni o popełnienie przestępstwa oraz obawa uznania takiej opinii za niedopuszczalną, z powodu tego, że przy jej opracowaniu wykorzystany został materiał dowodowy uzyskany w sposób niedozwolony. Zob. ibid.;
- ✓ potencjalny wpływ, jaki znajomość akt sprawy (np. informacji o tym, że oskarżony przyznał się do winy) może mieć na bezstronność biegłego (por. J. Wójcikiewicz: *Temida…*, op. cit., s. 194; B. Grabowska, A. Pietryka, M. Wolny, A. Bodnar: *Raport HFPC…*, op. cit., s. 39).

W kryminalistyce, w porównawczych badaniach identyfikacyjnych przyjęły się pojęcia „materiału kwestionowanego" oraz „materiału porównawczego"[136]. Dotyczą one badań mających na celu ustalenie tożsamości osób bądź procesów, efektem działania których jest powstanie obu materiałów (czy odręczne napisy wykonała ta sama osoba, czy wydruki zostały wykonane na tej samej drukarce itd.). W przypadku opiniowania informatycznego badania takie dotyczą zazwyczaj identyczności zapisów w plikach bądź na nośnikach[137], oraz wykonania tzw. dokumentów elektronicznych przy użyciu konkretnego urządzenia (np. zdjęć wykonanych cyfrowym aparatem fotograficznym[138]).

Jak wspomniano wcześniej, w polskim systemie prawnym biegły nie pełni roli „sędziego faktu", stąd też celem opinii biegłego nie powinno być ani „wyrokowanie", ani „orzekanie" na temat okoliczności faktycznych czy na temat ich konsekwencji prawnych. Opinia biegłego nie powinna służyć sądowi do ustalenia okoliczności faktycznych, to bowiem pozostaje domeną organu procesowego[139]. Nie można jednak nie zauważyć, że bardzo czę-

[136] Zob. np.: J. Wójcikiewicz: *Ekspertyza…*, op. cit., s. 28 i nast.

[137] Warto pamiętać, że badania wydruków komputerowych nie są badaniami informatycznymi, ale pismoznawczymi. Kompetentny do ich wykonania będzie zatem biegły z zakresu pismozawstwa.

[138] Warto zwrócić uwagę, że organy procesowe stosunkowo często nieprecyzyjnie formułują pytania dotyczące tego rodzaju dowodów. O ile przy wykorzystaniu narzędzi informatycznych jest możliwe – zbadanie obecności pewnych charakterystycznych cech aparatu obecnych na zdjęciu (m.in. rozkładu szumów będących efektem nierównomierności, zabrudzeń matrycy czy metadanych plików graficznych) i wydanie na tej podstawie opinii (o różnym stopniu stanowczości konkluzji) o tym, czy zdjęcie zostało wykonane badanym aparatem i nie zostało później przetworzone, o tyle informatyk nie jest kompetentny do oceny tego, czy sytuacja przedstawiona na zdjęciu odpowiada rzeczywistości.

[139] Istnieje na ten temat bogate orzecznictwo. Między innymi:

- ✓ Sąd Najwyższy w wyroku z 11 lipca 1969 r. (I CR 140/69) stwierdził: „Opinia biegłego ma na celu ułatwienie sądowi należytej oceny zebranego w sprawie materiału wtedy, gdy potrzebne są do tego wiadomości specjalne. Nie może ona natomiast sama być źródłem materiału faktycznego sprawy ani tym bardziej stanowić podstawy ustalenia okoliczności będących przedmiotem oceny biegłego" oraz: „Zadaniem biegłego nie jest ustalenie stanu faktycznego sprawy, lecz naświetlenie i wyjaśnienie przez sąd okoliczności z punktu widzenia posiadanych przez biegłego wiadomości specjalnych przy uwzględnieniu zebranego i udostępnionego biegłemu materiału sprawy";

- ✓ Wojewódzki Sąd Administracyjny we Wrocławiu w wyroku z 11 marca 2009 r. (II SA/Wr 251/08) stwierdził: „Celem dowodu z opinii biegłego (…) nie jest (…) ustalenie faktów mających znaczenie dla rozstrzygnięcia sprawy, lecz jedynie udzielenie organowi administracji publicznej wyjaśnień niezbędnych do rozstrzygnięcia sprawy. (…) Opinia biegłego stanowi bowiem jedynie ocenę grupy faktów przy użyciu ustawowych lub subiektywnych kryteriów opiniującego, dotyczącą stanu faktycznego dokonaną przez naświetlenie i wyjaśnienie okoliczności wskazanych przez organ administracji z punktu widzenia posiadanych przez biegłego wiadomości specjalnych. Opinia ta, nie może jednak zastąpić swobodnej oceny dowodów oraz ustalenia przesłanek wymaganych przepisami prawa materialnego. To do organu procesowego należy rozpatrzenie wszystkich okoliczności sprawy i podjęcie wszelkich niezbędnych kroków w celu dokładnego wyjaśnienia stanu faktycznego oraz ustalenia prawdy obiektywnej, a także subsumpcja faktu uznanego za udowodniony pod stosowną normę prawną i prawidłowe ustalenie następstw prawnych faktu uznanego za udowodniony na podstawie stosownej normy prawnej”;
- ✓ w wyroku z 11 lipca 1969 r. (I CR 140/69) Sąd Najwyższy stwierdził, że: „Opinia biegłego ma na celu ułatwienie sądowi należytej oceny zebranego w sprawie materiału wtedy, gdy potrzebne są do tego wiadomości specjalne. Nie może ona natomiast sama być źródłem materiału faktycznego sprawy ani tym bardziej stanowić podstawy ustalenia okoliczności będących przedmiotem oceny biegłego”;
- ✓ według postanowienia Sądu Najwyższego z 7 lipca 2005 r. (V KK 91/05) „Nie jest zadaniem biegłych odtworzenie faktów istotnych dla rozstrzygnięcia sprawy. Obowiązek ten spoczywa na sądzie orzekającym, przy czym opinie biegłych mogą okazać się *in concreto* dowodami wydatnie ułatwiającymi jego wypełnienie”;
- ✓ Sąd Najwyższy w wyroku z 6 lutego 2003 r. (IV CKN 1763/00) stwierdził: „Zadaniem biegłego jest udzielenie sądowi, na podstawie posiadanych wiadomości fachowych i doświadczenia zawodowego, informacji i wiadomości niezbędnych do ustalenia i oceny okoliczności sprawy. Nie mogą być uznane za dowód w sprawie wypowiedzi biegłego wykraczające zarówno poza zakres udzielonego mu przez sąd zlecenia, jak i poza ustawowo określone jego zadania. Sąd nie jest więc związany opinią biegłego w zakresie jego wypowiedzi co do – zastrzeżonych do wyłącznej kompetencji sądu – kwestii ustalenia i oceny faktów oraz sposobu rozstrzygnięcia sprawy”;
- ✓ w postanowieniu z 7 listopada 2000 r. (I CKN 1170/98) Sąd Najwyższy stwierdził: „Przedmiotem opinii biegłego nie jest przedstawienie faktów, lecz ich ocena na podstawie wiedzy fachowej (wiadomości specjalnych). Nie podlega ona zatem weryfikacji, jak dowód na stwierdzenie faktów, na podstawie kryterium prawdy i fałszu. Nie są miarodajne dla oceny tego dowodu niekonkurencyjne z nim oceny świadków i uczestników postępowania co do faktów będących przedmiotem opinii”.

sto samo ustalenie faktu wymaga wiedzy specjalistycznej[140] (w przypadku opiniowania informatycznego jest to wręcz sytuacja standardowa), stąd też powołanie się na zacytowane wcześniej orzeczenia sądów przez biegłego, któremu organ procesowy zadał pytanie o stan faktyczny, nie jest zazwyczaj skuteczne. Co więcej – niektóre opinie z natury rzeczy sprowadzają się do ustalania stanów faktycznych[141]. Formułując opinię należy jednak unikać sytuacji, w której można by odnieść wrażenie, że biegły autorytatywnie „orzeka" o zaistniałych stanach faktycznych[142], a tym bardziej o ich prawnych implikacjach, zgodnie bowiem z zasadą *iura novit curia*, ustalenie stanu prawnego i jego konsekwencji należy do organu procesowego i biegły nie może go w tym zadaniu wyręczać[143]. Nie oznacza to jednak, aby pomoc biegłego nie miała znaczenia już na etapie subsumpcji czynu zabronionego; wręcz przeciwnie jest ona szczególnie potrzebna w przypadku przestępstw komputerowych (hackingu, sabotażu komputerowego, oszustwa komputerowego itd.), gdzie kwalifikacja czynu może być niejednokrotnie wątpliwa[144] i organ procesowy może, a nawet powinien, posiłkować się opinią

[140] Zob. np.: H. Pietrzkowski: *Zarys metodyki pracy sędziego w sprawach cywilnych*, LexisNexis, Warszawa 2006.

[141] Na przykład rekonstrukcja wypadku drogowego. Por. np. R. Zahorski: *Metodyka*…, op. cit.

[142] Nie oznacza to, że nie można wydawać w tym zakresie opinii z wnioskami stanowczymi, czym innym jest jednak stwierdzenie, że – na przykład – awaria komputera spowodowana była niewłaściwym podłączeniem zasilania, a czym innym, że oskarżony rozmyślnie uszkodził komputer podłączając zasilanie w sposób niewłaściwy, przez co doprowadził do poniesienia przez pokrzywdzonego strat o wielkiej wartości.

[143] Na ten temat sądy wypowiadały się wielokrotnie, np.:

- ✓ Sąd Najwyższy w wyroku z 12 listopada 1973 r. (II KR 285/72): „Nie jest rzeczą biegłego wyjaśnianie sądowi treści obowiązujących w danej dziedzinie przepisów prawnych, gdyż w tym zakresie sąd jako organ stosujący prawo ma obowiązek samodzielnie czynić ustalenia w drodze bezpośredniego zapoznania się z treścią przepisów";
- ✓ Naczelny Sąd Administracyjny, Ośrodek Zamiejscowy w Łodzi, w wyroku z 3 października 2003 r., (I SA/Łd 2414/2001): „Biegły nie może być powołany w celu ustalenia obowiązującego prawa, zasad jego wykładni lub stosowania. W przeciwnym wypadku opinia biegłego zastępowałaby orzeczenie organu właściwego do wydania rozstrzygnięcia".

Zob. też K. Pachnik: *Dowód z opinii biegłego w prawie polskim*, http://www.ora.warszawa.com.pl/uploaded/Dow%C3%B3d%20z%20opinii%20bieg%C5%82ego%20w%20prawie%20polskim.pdf.

[144] Jako przykład można podać jedną ze spraw karnych opiniowanych przez autora artykułu, w której w trakcie postępowania przygotowawczego (śledztwa) trzykrotnie zmieniano

osoby posiadającej wiadomości specjalne, ale opinie takie powinny mieć charakter pomocniczy i nie zawierać w sobie propozycji kwalifikacji prawnej czynu, ale co najwyżej wskazywać na okoliczności, które mogą być dla dokonania takowej, zdaniem biegłego, istotne[145].

Od zasady tej istnieje kilka wyjątków: możliwe jest tworzenie opinii prawnych dla Trybunału Konstytucyjnego, biegły może wypowiadać się w kwestiach prawnych w kilku szczególnych wypadkach (gdy idzie o kwestie prawa obcego, bądź specjalizowanej gałęzi prawa[146], jak również o prawo zwyczajowe). W odniesieniu do biegłych informatyków spotyka się czasami opinie dotyczące prawa autorskiego do programów komputerowych w zakresie wymogów licencyjnych poszczególnych producentów. Zalecana jest w takim przypadku duża powściągliwość i ograniczenie się biegłego do ewentualnego informowania sądu o tym, jakie są warunki licencyjne stawiane przez producenta i gdzie można je znaleźć, natomiast stanowczo niepoprawne metodologicznie jest niestety spotykane w opiniach biegłych – stanowcze wnioskowanie na temat naruszenia wymogów licencyjnych[147].

3.3 Błędy w pytaniach do biegłych informatyków

Zakres opinii, jak napisano powyżej, dany jest poleceniem i pytaniami organu procesowego. Jeśli polecenie to bądź pytania są niewłaściwie sformu-

klasyfikację popełnionego czynu, ostatecznie zaś sąd, w trakcie procesu karnego, zmienił ją po raz czwarty (kwalifikując zresztą czyn nie jako przestępstwo, ale jako wykroczenie).

[145] W wyroku z 20 maja 1997 r., (I SA/Łd 345/96) Naczelny Sąd Administracyjny, Ośrodek Zamiejscowy w Łodzi stwierdził: „Żaden przepis prawa nie zabrania organom podatkowym subsydiarnego wykorzystania opinii biegłego do spraw rachunkowości i księgowości, którego zadaniem nie będzie oceniać prawa, lecz dopomóc w ustaleniu rzeczywistego obrazu rachunkowości".

[146] W wyroku Naczelnego Sądu Administracyjnego – Ośrodek Zamiejscowy w Lublinie z 19 lutego 1999 r. (SA/Lu 43/98) sąd stwierdził: „Opinia prawna wydana przez niezależnego prawnika, specjalizującego się w określonej dziedzinie (prawie autorskim), była w świetle art. 75 § 1 KPA dopuszczalnym dowodem pozwalającym na pełniejszą ocenę istotnych dla rozstrzygnięcia sprawy okoliczności".

[147] Zob. np.: P. Waglowski: *Secondlife: gdy organy ścigania stawiają zarzut za darmowy program*, http://prawo.vagla.pl/node/8138.

łowane, niemożliwe jest wykonanie prawidłowej opinii. Mówiąc o błędach w pytaniach do biegłych, należy rozróżnić przynajmniej trzy sytuacje[148]:

1) pytania źle postawione z formalnologicznego punktu widzenia;
2) pytania sformułowane w sposób niejasny, bądź zawierające wtrącone nieprawdziwe zdania;
3) pytania, na które odpowiedź byłaby przekroczeniem zakresu kompetencji biegłego (a w skrajnym przypadku nawet przepisów prawa).

Ad 1) Z formalnologicznego punktu widzenia pytanie nie jest zdaniem, nie może więc być ani fałszywe, ani pozbawione sensu. W logicznej teorii pytań wyróżnia się natomiast tzw. pytania źle postawione. W szczególności do pytań takich zalicza się pytania z fałszywym założeniem (presupozycją), np. „Czy przestał Pan już bić matkę?" zadane komuś, kto nigdy matki nie bił. Oczywiście poprawną odpowiedzią na takie pytanie jest zanegowanie presupozycji („nigdy nie biłem matki"), natomiast zadawanie takich pytań (przekazujących jakąś – nieprawdziwą – informację) jest w warunkach postępowania sądowego elementarnym błędem, niemniej można się z takimi pytaniami do biegłych spotkać. Czasami wynika to z niezrozumienia przez stronę jakichś szczegółowych kwestii, natomiast jako co najmniej etycznie wątpliwe należy ocenić próby stosowania tego rodzaju pytań jako sugestii służących do manipulowania biegłym, stosowane czasem przez strony postępowania.

Problematyczne jest zadawanie pytań z presupozycją, której wartość logiczna jest w chwili zadawania pytania nieznana. Dotyczy to w szczególności zjawiska quasi-uwiarygodniania zeznań świadków przez opinię biegłych. W – skrajnie uproszczonym – przykładzie świadek (którego prawdomówność podlega przecież swobodnej ocenie organu procesowego) zeznaje, że oskarżony uszkodził system komputerowy. Prokurator zadaje biegłemu pytanie „proszę

[148] Tomaszewski definiuje trzy rodzaje uchybień w pytaniach do biegłych: zbytnia ogólnikowość lub niepełność pytań, żądanie odpowiedzi wychodzących poza kompetencje biegłych, stawianie pytań, na które nie można udzielić odpowiedzi (zob. T. Tomaszewski: *Dowód z opinii biegłego w procesie karnym*, IES, Kraków 1998, s. 71 i nast.).

wyjaśnić charakter dokonanych przez oskarżonego uszkodzeń systemu komputerowego" (zamiast „proszę wyjaśnić charakter uszkodzeń systemu komputerowego"), aby potem konkludować, że „zgodnie z zeznaniami świadka i opinią biegłego uszkodzenia dokonane przez oskarżonego miały taki to a taki charakter" (zatem: to oskarżony dokonał uszkodzeń, bo tak mówili zgodnie i świadek, i biegły). Z formalnego punktu widzenia, odpowiedź na tak zadane pytanie wymagałaby wydania przez biegłego opinii alternatywnej („jeżeli sąd zechce uznać zeznania świadka za prawdziwe, to charakter tych uszkodzeń był taki to a taki, w przeciwnym razie pytanie jest pytaniem źle postawionym, z fałszywą presupozycją"). Oczywiście w rzeczywistości sytuacje takie są znacznie bardziej złożone i znacznie bardziej subtelne (szczególnie jeśli występują sprzeczne zeznania świadków, wówczas biegły może otrzymać od stron pytania z presupozycjami wzajemnie się wykluczającymi). Stąd też należy pamiętać, że nie jest rolą biegłego wyręczanie organu procesowego w ocenie materiału dowodowego oraz że opinia biegłego nie może być źródłem materiału faktycznego. Biegły może i powinien natomiast poinformować organ prowadzący postępowanie, jakie są konieczne konsekwencje uznania za prawdziwe treści jednego bądź drugiego z wykluczających się zeznań (dokumentów), o fakcie, że treść zeznań (dokumentów) pozostają w sprzeczności ze sobą, bądź z ustaleniami dyscypliny, którą biegły reprezentuje; sam organ procesowy, nie dysponując wiadomościami specjalnymi, może bowiem takiej sprzeczności nie dostrzec.

Ad 2) Jednym z podstawowych problemów, na które napotyka biegły w kontaktach z sądem, są trudności wynikające z użycia kilku różnych dialektów (języków): języka specjalności reprezentowanej przez biegłego, języka prawnego (języka aktów prawnych), języka prawniczego (którym prawnicy rozmawiają o prawie) i wreszcie – języka potocznego. Stąd też szczególną uwagę należy zwrócić na te pojęcia (nazwy), które występują jednocześnie w różnych językach, a którym odpowiadają różne desygnaty i zakresy pojęciowe, przy korzystaniu bowiem z tych pojęć najłatwiej jest o pomyłki i nieporozumienia, które mogą mieć bardzo daleko idące konsekwencje.

Ponieważ pierwszeństwo w komunikacji biegłego z sądem należy do tego drugiego (to sąd bowiem formułuje jako pierwszy pytanie do biegłego), to rolą biegłego jest starać się zrozumieć język organu procesowego[149]. Dobrym zwyczajem (ze strony prawników) jest skorzystanie przez prawnika przy układaniu pytań z pomocy osoby, która potrafi posłużyć się fachowym językiem[150]. Jeśli jednak pytanie zadane biegłemu jest niejasne czy niezrozumiałe, zdecydowanie powinien on dążyć do jego wyjaśnienia, nie próbując samemu zgadywać, co zadający pytanie uczestnik postępowania miał na myśli.

Niezrozumiałe pytania, bądź pytania zawierające wtrącone nieprawdziwe zdania, są często efektem swoistego, źle rozumianego, krasomówstwa przedstawicieli procesowych stron, bądź niezrozumienia elementarnych pojęć odpowiedniej dyscypliny nauki czy techniki. Jako przykłady można podać kilka pytań przytoczonych w pracy Jolanty Jerzewskiej:

- ✓ „Czy daty utworzenia plików świadczą o ich systematycznym uzupełnianiu?”[151];

> Zadający pytanie miał zapewne na myśli pytanie, czy czasy utworzenia różnych plików są na tyle różne od siebie, żeby wyciągnąć stąd wniosek o ciągłości działania przestępnego (w tym wypadku mowa była o gromadzeniu zasobów pornografii dziecięcej). Rzecz jasna nie jest rolą biegłego wnioskowanie na temat „systematyczności” takiego działania (tym bardziej, że wykorzystanie metadanych zazwyczaj prowadzi do wniosków o niskiej stanowczości, z uwagi na wyjątkową ulotność metadanych: np. czas utworzenia pliku zmieni się przy przenoszeniu plików po-

[149] Jak pisze T. Widła: „Problem prawnika (wyrażony językiem prawniczym) nie jest problemem biegłego, bo wykonując ekspertyzę nie rozwiązuje on problemów prawniczych, nie myśli z użyciem języka prawniczego, a języka reprezentowanej specjalności (...). Biegły może rozwiązać problemy sformułowane tak, jak się to czyni w naukach przyrodniczych, ekonomicznych itp. Tak więc na wstępie biegły kwestię sformułowaną w języku prawniczym przekształcić musi na wyrażony w języku swej specjalności” (zob. J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 26).

[150] Na przykład z pomocy „biegłego prywatnego”.

[151] Zob. J. Jerzewska: *Od oględzin*…, op. cit., s. 153 (pytanie 70).

między wolumenami o różnych systemach plików). Prawidłowe byłoby po prostu żądanie od biegłego sporządzenia listy plików wraz z czasami MAC.

- ✓ „Czy zabezpieczony do badań komputer posiada modem lub kartę sieciową lub inne urządzenie do komunikacji z siecią komputerową? [Obecność modemu lub karty sieciowej sugeruje, że gromadzone treści były sprowadzane (rozpowszechniane) drogą elektroniczną. Z kolei dwie karty sieciowe zainstalowane w komputerze mogą sugerować, że stanowił on serwer dla większej liczby komputerów, tworząc lokalną podsieć. Warto wyjaśnić, że istotne będzie, czy komputer jest połączony z urządzeniami łączącymi go z sieciami rozległymi, takimi jak: *Router*, *Firewall*, *Proxy-Server* itp. Urządzenia te posiadają tzw. *MAC Adress*. Identyfikuje on urządzenie i pozostawia w sieci ślady. Wskazuje również na występowanie podsieci]”[152];

Liczba błędów i nieścisłości w tym pytaniu i jego objaśnieniu jest zaskakująco duża:

- o niezależnie od tego, czy komputer posiada, czy nie posiada interfejsów sieciowych zawsze informacja jest do niego wprowadzana drogą elektroniczną, w skrajnym przypadku za pośrednictwem urządzeń przetwarzających na postać elektroniczną sygnały mechaniczne (klawiatura) czy optyczne (skaner);
- o serwer (ang. *Server*, *service provider*) nie musi posiadać wielu interfejsów sieciowych. Rozwiązania, w których serwer pełni dodatkowo rolę *routera* segmentującego sieć (a nie podsieć) lokalną były raczej charakterystyczne dla małych sieci lokalnych w XX wieku;
- o adres fizyczny MAC[153] posiada każde urządzenie działające w II i wyższych warstwach modelu referencyjnego

[152] Zob. ibid., s. 153 (pytanie 64). Zapis w nawiasach kwadratowych jest w oryginale umieszczony w przypisie.

[153] Ang. *Media Access Control* (podwarstwa kontroli dostępu do medium transmisyjnego w standardzie IEEE 802.2). Nie należy mylić adresu MAC ze wspominanymi wyżej metadanymi MAC – pomimo identycznego akronimu są to zupełnie inne dane.

ISO/OSI, a więc w szczególności każda karta sieciowa. Pojęcie podsieci związane jest zazwyczaj z protokołem IP (a więc protokołem warstwy III tegoż modelu) i nie ma z adresowaniem fizycznym nic wspólnego. Niezależnie od tego, czy sieć jest podzielona na podsieci czy nie, a nawet, czy dany komputer pracował w sieci, czy też samodzielnie, urządzenia sieciowe w nim zainstalowane mają swoje MAC adresy;

- MAC adres nie pozostawia w sieci śladów. Informacje o MAC adresie nadawcy i odbiorcy poszczególnych ramek (ang. *frame*) przesyłanych w sieci są umieszczone w nagłówkach tychże ramek. Przechwycenie ramki pozwala ustalić jej adresata i nadawcę, z tym, że z uwagi na brak uwierzytelnienia adresów MAC w popularnych protokołach stosu protokołów TCP/IP, stosunkowo łatwo można sfałszować adres nadawcy, a więc wnioskowanie na podstawie zarejestrowanych adresów MAC[154] również ma ograniczoną stanowczość.

✓ „Czy w przekazanych do badań logach systemowych [logi systemowe są to najczęściej pliki tekstowe, w których zapisane są wiersz po wierszu przez system operacyjny określone wydarzenia] nie ma »dziur czasowych«? [To pytanie (i kolejne) może okazać się przydatne w przypadku zajścia okoliczności wprowadzenia do komputera »nieprawdziwych postaci« lub »martwych duszyczek« dla osiągnięcia korzyści majątkowych. Najczęściej manipulacji dokonuje pracownik firmy]”[155];

W rzeczywistości luki w zapisach logów systemowych świadczyć mogą przede wszystkim o usunięciu części zapisów przez włamywacza i są wskazówką do wykonania niskopoziomowej analizy dysku pod kątem wykrycia usuniętych zapisów, natomiast o dodawaniu sfałszowanych zapisów w programach księgowych może świadczyć rozbieżność

[154] Dzieje się tak np. w przypadków ataku ARP-spoofing czy MAC-flooding. Zob. np.: M. Szmit, M. Gusta, M. Tomaszewski: *101 zabezpieczeń przed atakami w sieci komputerowej*, Wydawnictwo Helion, Gliwice 2005, s. 22 i nast.

[155] Zob. J. Jerzewska: *Od oględzin*…, op. cit., s. 153 (pytanie 45). Zapis w nawiasach kwadratowych jest w oryginale umieszczony w przypisie.

pomiędzy datami wprowadzania zapisów (o ile te da się odtworzyć), a datami w tych zapisach umieszczonymi (np. jeśli w programie finansowo-księgowym w roku 2014 zapisano księgowanie faktury wystawionej w roku 2010).

A. Żygadło[156] przytacza polecenia takie jak:

- ✓ „Proszę określić sprzętową i programową konfigurację płyt CD";
- ✓ „Proszę ustalić IP dysku twardego";
- ✓ „Proszę ustalić, jakie osoby korzystały z komputera".

Ad 3) Osobną klasę błędów stanowią pytania, na które odpowiedź przekracza kompetencje biegłego. Należy zawsze pamiętać, że choć biegły jest osobowym źródłem informacji, to jego kompetencje zawężone są do dziedziny, dla której został ustanowiony. Nie jest zadaniem biegłego dzielenie się z sądem swoimi przemyśleniami na tematy ogólne czy na temat innych dyscyplin nauki, sztuki czy techniki, nawet jeśli posiada w ich zakresie formalne wykształcenie[157].

[156] A. Żygadło: *Pytania do i odpowiedzi biegłych sądowych* [w:] *IX seminarium naukowe: materiały seminaryjne*, Wyższa Szkoła Policji, Szczytno 2006, s. 173–190.

[157] Klasyfikacja dyscyplin naukowych, czy zawodów nie pokrywa się ze specjalnościami biegłych (wykaz tychże zresztą pozostaje nieustandaryzowany i zależy od decyzji Prezesa odpowiedniego Sądu Okręgowego). Zdarzają się zresztą również przypadki powoływania biegłych z takich dziedzin ludzkiej aktywności, których nie da się w żaden sposób zaliczyć do nauki, sztuki, czy techniki. Na przykład uchwała Sądu Najwyższego z 30 października 1985 r. (SN III CZP 59/85), powołując się na rozporządzenie Ministra Handlu Wewnętrznego i Usług z 23 kwietnia 1983 r. w sprawie oznaczania rodzajów rzemiosł, określenia uprawnień i kwalifikacji zawodowych wymaganych do ich wykonywania oraz pierwszeństwa kombatantów w uzyskiwaniu zezwoleń na wykonywanie rzemiosła (dalej RORRKZ), dopuszcza przeprowadzenie dowodu z opinii biegłego radiestety, odnotowano również przypadki wydania przez prokuraturę postanowień o zasięgnięciu opinii biegłego jasnowidza (zob. *Prokuratura powołuje jasnowidza Jackowskiego jako biegłego. Pierwszy taki przypadek w Polsce*?, http://wiadomosci.gazeta.pl/wiadomosci/1,114871,14000927,Prokuratura_powoluje_jasnowidza_Jackowskiego_jako.html) i choć przypadki powoływania przedstawicieli paranauk do roli biegłych wyjaśniających rzeczywistość w oparciu o metody tychże paranauk należy – z punktu widzenia nauki – ocenić jako zachowanie zgoła zabobonne, to nie sposób nie zauważyć, że może mieć miejsce powołanie biegłego w tak egzotycznym zakresie odnośnie do ustalenia zwyczajów, czy praktyk panujących w środowisku osób zajmujących się jakąś działalnością (paranaukową); można też upierać się, że jeśli jakaś grupa osób czerpie korzyści

Jako przykłady tego rodzaju można podać również kilka pytań przytoczonych przez Jerzewską:

- ✓ „Czy zabezpieczany do badań komputer zawiera chronione prawnie informacje?”[158]

Oczywiście, prokurator, czy policjant prowadzący postępowanie przygotowawcze, a tym bardziej sędzia prowadzący postępowanie sądowe, powinien być w kwestiach prawnych zdecydowanie lepiej zorientowany od biegłego informatyka, który nie może w sposób kompetentny wypowiadać się o prawnym statusie treści informacji przechowywanej w systemie komputerowym[159]. Poza tym prawnie chronione są choćby programy komputerowe (podlegają – przynajmniej te z nich, które są utworami – ochronie prawa autorskiego), dane osobowe (np. imiona, nazwiska, adresy email) odpowiedź na tak postawione pytanie musi być zatem niemal zawsze twierdząca.

Podobne błędy znajdują się w pytaniach[160]:

- ✓ „Czy w zabezpieczonym w mieszkaniu podejrzanego komputerze (dysku twardym, nośnikach danych informatycznych) znajdują się zapisy treści pornograficznych z udziałem małoletnich?”;
- ✓ „Czy na przekazanych do badań dyskach twardych znajdują się zasoby o treściach pornografii dziecięcej?”;

Pytania te powinny być skierowane do sądu bądź prokuratora, a pomocne w udzieleniu na nie odpowiedzi mogą

majątkowe z uprawiania jakieś – choćby i irracjonalnej – działalności, to np. dla celów statystycznych można tę działalność zaklasyfikować jako zawód.

Z drugiej strony zrozumiałe jest różnicowanie dyscyplin biegłych bardziej niż dyscyplin naukowych: pojęcie takie jak np. „ekonomista” jest bardzo szerokie, stąd konieczność odróżnienia np. specjalisty od marketingu, od specjalisty od księgowości i choć osoba posiadająca np. tytuł naukowy profesora nauk ekonomicznych i specjalizująca się w rachunkowości na pewno dysponuje o wiele większą niż przeciętna wiedzą również z innych dyscyplin ekonomicznych (np. ekonomiki przedsiębiorstw), to wypowiadając się jako biegły sądowy z zakresu księgowości nie powinna wykraczać poza granice specjalności, dla której została ustanowiona.

[158] J. Jerzewska: *Od oględzin*…, op. cit., s. 148 (pytanie 19).

[159] Por. A. Żygadło: *Pytania*…, op. cit.

[160] J. Jerzewska: *Od oględzin*…, op. cit., s. 148–154 (pytania odpowiednio 56 i 69).

być opinie biegłego seksuologa i antropologa (zobacz rozdział 5.1); informatyk nie ma bowiem oczywiście kompetencji do opiniowania o treści informacji w tym np. o wieku osób uwidocznionych na zdjęciach lub filmach, czy o pornograficznym charakterze tychże materiałów. Właściwe byłoby skierowanie do informatyka polecenia ujawnienia treści zdjęć np. poprzez jej wydrukowanie, ewentualnie poprzez nagranie w czytelnym formacie na nośniku CD lub DVD.

Nieszczęśliwe jest również sformułowanie pytania[161]:

- ✓ „Czy materiał w postaci zdjęć o charakterze pornografii dziecięcej znalazł się na dysku przypadkowo, czy został na nim zgromadzony (sprowadzony) i/lub przetwarzany w sposób świadomy?"

Takie postawienie pytania czyni z biegłego informatyka w jednym seksuologa, oceniającego treść informacji, antropologa, ustalającego wiek przedstawionych w materiale kwestionowanym osób, śledczego, ustalającego okoliczności jej zapisu, psychologa lub psychiatrę, oceniającego stan świadomości podejrzanego i sędziego, rozstrzygającego o wypełnieniu ustawowego znamienia przestępstwa (a przy okazji jeszcze jest przykładem pytania z presupozycją, domniemana prawdziwość której jest równoważna stwierdzeniu popełnienia przestępstwa). Biegły informatyk może – jak miało to miejsce w przytaczanym wcześniej przykładzie – co najwyżej podać czasy MAC poszczególnych plików, ich liczbę czy sposób ich rozmieszczenia na dysku – np. w katalogach uporządkowanych tematycznie – które to informacje mogą wskazywać na celowe (a nie „świadome") ich gromadzenie i przetwarzanie (ale już ten wniosek o celowym charakterze działania musi wyciągnąć nie biegły, ale organ procesowy).

Na marginesie warto przytoczyć lepsze sformułowanie pytania dotyczącego treści informacji, znajdujące się w in-

[161] Ibid., s. 153 (pytanie 57).

nym poradniku[162]: „Czy urządzenia lub nośniki zawierają informacje wskazujące o[163] ich użyciu do celów przestępczych?". Mimo że można mieć wątpliwości, czy pytanie takie nie rozszerza zanadto zakresu ekspertyzy, w ten sposób przynajmniej biegły nie jest zmuszany do ferowania wyroków i klasyfikacji treści, a jedynie do zasugerowania organowi prowadzącemu śledztwo konieczności zapoznania się z treścią informacji, którą ujawnił[164].

W dużej części przypadków niezręczności w formułowaniu pytań są efektem pośpiechu i zbyt daleko idących skrótów myślowych sędziego, policjanta, prokuratora, radcy czy adwokata reprezentującego stronę. Niejednokrotnie organ procesowy zakreśla w postanowieniu o powołaniu biegłego cel opinii przepisany z dyspozycji normy karnej (np. „Czy oskarżony w istotnym stopniu zakłócił automatyczne przetwarzanie lub przekazywanie danych informatycznych?"), do czego oczywiście biegły nie może się odnieść wprost, bowiem nie jest jego rolą wyręczanie sądu w wydawaniu wyroków. Niejednokrotnie pytania są na tyle ogólne, że sensowna odpowiedź na nie jest w ogóle niemożliwa[165].

---

[162] M.P. Krysiak: *Biegły (pytania do biegłych)*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2005, s. 87–88.

[163] Tak w oryginale. Oczywiście powinno być „wskazujące na ich użycie" lub „świadczące o ich użyciu".

[164] Gwoli ścisłości: organ procesowy lub prowadzący śledztwo powinien zapoznać się osobiście z całością ujawnionej informacji, jednak może to być w praktyce niewykonalne z uwagi na jej rozmiar. Współczesne nośniki danych pozwalają na przechowywanie setek tysięcy plików o rozmiarze liczonym w terabajtach. Przygotowanie choćby wydruku zawierającego podstawowe metainformacje o wszystkich plikach zawartych na przeciętnym dysku twardym wymagałoby niejednokrotnie zużycia tysięcy stron papieru. Z tego też względu rozsądnym postulatem jest, aby instytucje prowadzące postępowanie przygotowawcze zatrudniały specjalistów umiejących stosować techniki komputerowej analizy informacji zebranej na nośnikach mogących być dowodami przestępstw (zob. np.: A. Lach: *Prawnodowodowa problematyka zwalczania pedofilii i pornografii dziecięcej w internecie* [w:] *Materiały Seminarium Przestępczość Teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2004, s. 59–65).

[165] T. Tomaszewski (*Postanowienia*…, op. cit., s. 66–69) przytacza sytuację, następującej wymiany zdań między sądem a biegłym:

„Sąd postanowił zlecić wydanie opinii co do techniki i taktyki prowadzenia pojazdu przez oskarżonego na podstawie materiału z dochodzenia i rozprawy.

O ile mowa jest o drobnych kwestiach merytorycznych, biegły może w ramach opinii dokonać uściślenia, czy nawet stosunkowo obszernej prezentacji rzeczywistego stanu wiedzy, choć wymaga to od niego zarówno wiedzy merytorycznej, jak i kompetencji osobistych (asertywności, taktu, umiejętności zachowania się w sytuacjach konfliktowych), o tyle w kwestiach poważnych nie zawsze udaje się uniknąć konfliktów pomiędzy biegłym a organem procesowym. Niestety praktyka pokazuje, że przynajmniej niektóre instytucje wymiaru sprawiedliwości mają skłonność do preferowania biegłych „bezkonfliktowych" dostarczających „jednoznaczne" opinie umożliwiające szybkie zakończenie sprawy. Efektem są często opinie zawierające odpowiedzi równie, a nawet bardziej bezsensowne czy niejasne, jak pytania, na które odpowiadają[166]. Jeszcze gorszą sytuacją, która niestety zdarza się – na szczęście raczej sporadycznie – w wymiarze sprawiedliwości są tacy gospodarze postępowania, którzy usiłują nakłonić biegłego do wydania opinii na temat legalności takiego czy innego zachowania oskarżonego *per fas et nefas*, powołując się na obowiązki biegłego, w tym przepisy dotyczące odpowiedzialności karnej za wydanie niezgodnej z prawem opinii. Autorowi znane są przypadki, w których biegli dołączali do pisemnej opinii biegłego opinię prawną wyjaśniającą, dlaczego odpowiedź na pytania zadane przez prowadzącego postępowanie byłaby niezgodna z prawem, czy nagrywali rozmowy prowadzone z prowadzącym postępowanie, aby udokumentować fakt wywierania na nich nacisków. Tego rodzaju sytuacje są oczywiście głęboko

Po przeanalizowaniu obecnego stanu sprawy (...) dochodzę do wniosku, że taktyka i technika prowadzenia samochodu przez oskarżonego była nieprawidłowa".

[166] Szerokim echem w środowisku biegłych odbiła się wypowiedź dr. Jerzego Pobochy na 1 Kongresie Nauk Sądowych, gdzie sformułował on „zasadę WIELOBE": organa wymiaru sprawiedliwości często potrzebują opinii wykonanych na zasadzie byle szybko, byle tanio otrzymują więc byle co, wykonane byle jak. Por. np. T. Widła, M. Leśniak: *Chytrze bydlą z pany kmiecie…*, Międzynarodowa Konferencja z okazji 55-lecia powstania Laboratorium Kryminalistycznego KWP w Krakowie, http://konferencjalkkwp.weebly.com/abstrakty.html.

patologiczne, niemniej – jeśli wierzyć literaturze przedmiotu – zdarzają się również biegłym innych specjalności[167].

3.4 Dopuszczalność metod i narzędzi badawczych

W literaturze poświęconej opiniowaniu[168] stosunkowo dużo miejsca, ze zrozumiałych względów, poświęca się kryteriom dopuszczalności poszczególnych metod pracy biegłego oraz zasadom ich oceny. W tym kontekście przywołuje się amerykański standard, tzw. standard Daubert[169]. Według tego stanowiska opinia powinna spełniać szereg kryteriów pozwalających ocenić, czy ekspertyza biegłego (konkluzje i badania) ma charakter naukowy. W oryginalnym wyroku kryteria te zostały omówione w sposób opisowy, w literaturze przedmiotu przedstawiane są zazwyczaj jako lista kilku elementów np.:

- ✓ „sąd sformułował zatem następujące kryteria oceny dowodu naukowego: falsyfikacji, recenzji, publikacji, wartości diagnostycznej (znany lub potencjalny poziom błędu), standaryzacji, powszechnej akceptacji”[170];
- ✓ „po pierwsze, zastosowana metoda badawcza została przetestowana lub jej testowanie jest możliwe w przyszłości. Warunek ten wyklucza wszelkie metody, które potencjalnie nie mogą być testowane empirycznie (np. wróżenie z fusów, rozmowa z duchami, czytanie z kart). Po drugie, opis metody i osiągane za jej pomocą re-

[167] Kilka tego rodzaju przypadków omówionych jest też np. w pracy Z. Marek: *Wybrane*…, op. cit.

[168] Zob. np.: J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 20 i nast.

[169] Kryteria wypracowane przez Sąd Najwyższy Stanów Zjednoczonych w trzech sprawach:

- ✓ Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993) http://supreme.justia.com/cases/federal/us/509/579/case.html oraz w sprawie apelacyjnej (Daubert v. Merrell Dow Pharmaceuticals, Inc., 43 F. 3d 1311 – Court of Appeals, 9th Circuit 1995 http://law.justia.com/cases/federal/appellate-courts/F3/43/1311/552448);
- ✓ General Electric Co. v. Joiner, 522 U.S. 136 (1997) http://supreme.justia.com/cases/federal/us/522/136/case.html;
- ✓ Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999) http://supreme.justia.com/cases/federal/us/526/137/case.html,

które uzupełniły i zastąpiły wcześniejsze kryteria Frye z 1923 r.

[170] J. Wójcikiewicz*: Ekspertyza*…, op. cit., s. 21.

zultaty zostały opublikowane i poddane recenzji środowiska naukowego. Po trzecie, znany jest margines potencjalnego błędu pojawiającego się w badaniach z wykorzystaniem określonej techniki. Po czwarte, dana metoda badawcza powinna cieszyć się akceptacją środowiska naukowego. (…) Cztery lata później (…) »standard Daubert« został wzbogacony przez dodatkowe zalecenie w sprawie General Electric Co. v. Joiner. Sądy powinny poddawać szczegółowej analizie nie tylko konkluzje wynikające z opinii naukowej, ale również proces rozumowania, który za nią stoi"[171];

- ✓ „(…) aby jakakolwiek technika lub metoda została uznana za dowód naukowy, musi spełniać cztery warunki: a) musi być sama w sobie sprawdzalna i była już poddana takiej procedurze, b) była opisana w literaturze fachowej, c) jest znany (a co najmniej przewidywany) procent błędnych rozstrzygnięć uzyskiwanych przy zastosowaniu tej metody, d) metoda uzyskała powszechną akceptację specjalistów danej dziedziny"[172].

Jak widać pewnym problemem jest tu pojęcie empirycznej sprawdzalności metody. Nie jest przecież tak, aby owego „wróżenia z fusów" nie dało się testować empirycznie. Da się to oczywiście wykonać, z tym, że rezultat takich testów będzie – jak można się spodziewać – negatywny. Możliwość empirycznego testowania metody nie jest jednak tożsama z weryfikowalnością tej metody. Nie da się np. empirycznie (doświadczalnie) testować choćby twierdzeń logiki, które jednak niewątpliwie mają charakter naukowy, w szczególności są intersubiektywnie weryfikowalne[173]. Falsyfikacja wreszcie, rozumiana tak, jak rozumiał ją cytowany zresztą w powołanym wyroku Popper, dotyczy oczywiście nie falsyfikacji (stwierdzenia

[171] R. Zyzik: *Dowody neuronaukowe w polskim prawie dowodowym*, „Forum Prawnicze" 2013, vol. 2 (16), s. 23–34, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2337387.

[172] J. Widacki [w:] *Kryminalistyka*, pod red. J. Widackiego, C.H. Beck, Warszawa 2008.

[173] Jakieś zdanie wtedy jest weryfikowalne, gdy można je albo zweryfikować, albo sfalsyfikować, tzn. jeżeli można pokazać, że jest ono prawdziwe albo, że jest ono fałszywe. Oczywiście w odniesieniu do twierdzeń matematycznych odnosi się to do prawdziwości w obrębie pewnej aksjomatyki – zob. J. Bocheński: *Współczesne metody myślenia*, W drodze, Poznań 1988, s. 41.

nieprawdziwości)[174] użytej przez biegłego metody, czy dokładniej: teorii, w oparciu o którą powstała (podówczas wróżenie z fusów należałoby uznać za metodę dopuszczalną, bo sfalsyfikowaną), ale sposobu rozwoju danej dyscypliny nauki[175]. Za słuszną więc należy uznać krytykę tego kryterium podaną w powołanej pracy Józefa Wójcikiewicza[176].

W formalnej postaci kryteria stosowalności metod naukowych w Stanach Zjednoczonych zostały zebrane w Federalnej Regule Dowodowej 702:

„Reguła 702. Zeznania biegłych[177]

Świadek, który został zakwalifikowany jako ekspert, dzięki posiadanej wiedzy, umiejętności, doświadczeniu, szkoleniu, czy wykształceniu, może zeznawać w formie opinii lub w inny sposób, jeżeli:

1) wiedza naukowa, techniczna lub inna wiedza specjalistyczna eksperta pomogą sędziemu faktu[178] zrozumieć dowody lub ustalić fakt w sprawie;

---

[174] Gwoli ścisłości: powinno się tu mówić o falsyfikowalności, a nie falsyfikacji (podobnie należy rozróżnić weryfikację od weryfikowalności).

[175] „Jeżeli zdanie wyjaśniające zostało już redukcyjnie sformułowane, wtedy następnym etapem jest zwykle tzw. weryfikacja, tzn. zdanie to próbuje się potwierdzić albo odrzucić za pomocą redukcji progresywnej. Dzieje się to w następujący sposób: ze zdania sformułowanego na drodze redukcji wyprowadza się, w oparciu o system aksjomatyczny (który zwykle nie jest czysto logiczny, lecz zawiera także wiele redukcyjnie utworzonych zdań), nowe zdania, które w odpowiedniej dziedzinie są bezpośrednio weryfikowalne, tzn. których wartość prawdziwościowa da się stwierdzić. Następnie przeprowadza się operacje (eksperymenty itd.) wymagane, aby móc ustalić wartość prawdziwościową wyprowadzonych zdań. Jeżeli okaże się, że są one prawdziwe, wtedy uzyskuje się konfirmację zdania, z którego zostały one wyprowadzone. Jeżeli okazuje się jednak, że są one fałszywe, wtedy mówi się o falsyfikacji: w tym wypadku zdanie, z którego zostały one wyprowadzone odrzuca się jako fałszywe.

Ma tu miejsce uderzająca asymetria. Falsyfikacja jest logicznie konkluzywna, natomiast konfirmacja nigdy nie jest ostateczna, gdyż jak już powiedzieliśmy, wnioskowanie z następnika o poprzedniku nie jest niezawodne, podczas gdy wnioskowanie z negacji następnika o negacji poprzednika jest uzasadnione przez prawo logiczne i obowiązuje ogólnie. W związku z tą sytuacją twierdzono, że nauki redukcyjne rozwijają się właściwie nie przez pozytywne, lecz przez negatywne kroki, wykluczając jedno po drugim fałszywe wyjaśnienia za pomocą falsyfikacji". J. Bocheński: *Współczesne*..., op. cit., s. 7–8.

[176] J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 22.

[177] Przyp. aut.: dosł. „uczonych świadków" – jest to związane z systemem prawa amerykańskiego, w którym rola procesowa biegłego jest właśnie rolą uczonego świadka (por. rozdział 2.4).

[178] Przyp. aut.: dosł. *trier of fact*. Jest to konstrukcja związana z rolą, jaką pełni sąd w systemie prawa amerykańskiego (por. VII poprawka do Konstytucji Stanów Zjednoczonych).

2) zeznanie to opiera się na odpowiednich faktach lub danych;
3) zeznanie to jest wynikiem wiarygodnych zasad i metod oraz
4) ekspert w sposób godny zaufania zastosował te zasady i metody do okoliczności sprawy[179]".

W realiach polskich nie obowiązuje formalna teoria dowodów (zob. rozdział 3.7), zaś orzecznictwo dotyczące metod badawczych dopuszczalnych w procesie opiniowania jest stosunkowo ubogie[180]. Wyroki Sądu Najwyższego podkreślają rolę powszechnej akceptacji metod badawczych, kryterium aktualnego stanu wiedzy czy obecnego stanu nauki. W praktyce uniemożliwia to stosowanie do celów opiniodawczych metod o nieugruntowanej pozycji naukowej, pionierskich[181].

Należałoby zastanowić się, jak z punktu widzenia tych reguł wygląda opiniowanie informatyczne. W szczególności wątpliwości może budzić weryfikowalność wyników otrzymanych za pomocą niektórych narzędzi informatycznych. Biegły posługując się programami komputerowymi, w szczególności programami specjalistycznymi, o zamkniętym kodzie, często narzędziami przeznaczonymi do analizy specyficznego rodzaju zapisów w nieudokumentowanych formatach przypisanych do konkretnej wersji oprogramowania użytkowego (np. klientów usług P2P czy specyficznych komunikatorów internetowych), nie ma możliwości przeprowadzenia innych – niż bardzo wyrywkowe – testów poprawności działania narzędzi. Nie może wykluczyć, że w procesie przetwarzania danych pewne z nich

[179] „Rule 702. Testimony by Expert Witnesses
A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:
1) the expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;
2) the testimony is based on sufficient facts or data;
3) the testimony is the product of reliable principles and methods and
4) the expert has reliably applied the principles and methods to the facts of the case",
http://www.law.cornell.edu/rules/fre/rule_702 (jest to wersja reguły po uzupełnieniu z 1 grudnia 2011 r.).

[180] Zob. J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 21 i nast.

[181] Przez szereg lat z problemami takimi borykała się osmologia, obecnie pełnoprawna technika kryminalistyczna ze stosunkowo dobrze rozwiniętymi standardami wykonywania badań i opiniowania.

zostaną przez program pominięte lub źle zinterpretowane[182]. Powyższe uwagi nie mają na celu podważania metodologicznej poprawności opinii informatycznych ani ich wiarygodności dowodowej, a jedynie zwrócenie uwagi na fakt, że stosowane metody (i narzędzia) badawcze powinny być w miarę możliwości przetestowane i godne zaufania[183], zaś biegły powinien być rzeczywiście biegły w ich użyciu, w tym w interpretacji otrzymanych wyników[184].

---

[182] Może to mieć miejsce nawet w sposób zamierzony przez twórcę oprogramowania: podejrzewa się np., że część programów typu *internet security* celowo nie wykrywa narzędzi szpiegujących wykorzystywanych przez różnego rodzaju służby specjalne. Warto wspomnieć także o narzędziach *antiforensic*, które mają za zadanie utrudnić bądź zaburzyć proces akwizycji i analizy danych wykonywany popularnymi programami stosowanymi przez informatyków śledczych. Narzędzia te dzielą się na kilka klas – obok standardowych programów usuwających trwale zapisy z dysków czy szyfrujących ich zawartość, również programy fałszujące zapisy czy reagujące na obecność w systemie określonych programów. Jako przykłady można podać program DECAF z końca lat 90. ubiegłego wieku (http://en.wikipedia.org/wiki/DECAF), który wykrywał zestaw narzędzi COFEE (opracowany przez Microsoft zestaw narzędzi do badań typu *live forensic* udostępnianych organom ścigania) i w razie stwierdzenia jego obecności uruchamiał zdefiniowane przez użytkownika procesy, takie jak np. odłączanie dysku USB, na którym znaleziono COFEE, czy *attention-deficit-disorder* (https://code.google.com/p/attention-deficit-disorder/) – program typu *proof-of-concept*, służący do fałszowania zawartości pamięci RAM.

[183] Na marginesie uwag o metodach i narzędziach badawczych biegłego informatyka należy przypomnieć o konieczności użycia sprzętowych blokerów zapisu analizowanych nośników pamięci masowej, wszędzie tam, gdzie jest to możliwe (zob. Załącznik). Prowadzenie badań na niezabezpieczonym nośniku prowadzi do kontaminacji materiału badawczego i w konsekwencji staje się przyczyną niemożliwości wydania opinii (zob. rozdział 2.4.1).

[184] W szczególności warto zwrócić uwagę na kwestie elementarne: np. w jakim standardzie podawane są przez programy informacje o czasie (np. o czasie wpisu w logach systemowych). Może to być czas UTC albo lokalny czas komputera (tego, na którym logi utworzono, albo tego, na którym prowadzone jest badanie), ponieważ nie ma tu jednolitego standardu wyniki otrzymane różnymi programami mogą różnić się od siebie. Innym trywialnym źródłem błędów jest traktowanie (przez programy do wykonywania kopii i obliczania sum kontrolnych) bloków dysku niemożliwych do odczytania (zazwyczaj są one uzupełniane jakimś zapisem, np. zerami albo spacjami albo napisem zdefiniowanym przez użytkownika programu np. „UNREADABLE SECTOR"). Oczywiście różne wypełnienia będą prowadziły do obliczenia różnych sum kontrolnych, co może prowadzić do podważenia wiarygodności wykonanej kopii. Należy również poprawnie interpretować nazewnictwo używane w programach użytkowych, niestety nie zawsze jednoznaczne, np. sektor dysku (ang. *sector*) to nie to samo co blok (ang. *block*), zaś partycja dysku (ang. *parti-*

Z kwestią dopuszczalności metod i narzędzi badawczych jest związane zagadnienie wyboru metody badawczej (o ile oczywiście postawiony problem taki wybór umożliwia). Kwestia ta należy do zakresu objętego tzw. autonomią biegłego[185]: racjonalny wybór metody badawczej jest możliwy wyłącznie wtedy, jeśli osoba dokonująca tego wyboru posiada odpowiednie wiadomości specjalne z zakresu dyscypliny, do których możliwe metody należą[186].

Przepisy kodeksowe nie wskazują możliwości nakazania biegłemu wykonania badania wskazaną przez organ procesowy metodą, również orzecznictwo wskazuje, że wybór metody jest kwestią biegłego[187]. Jak słusznie pi-

tion) to nie to samo co umieszczony na niej dysk logiczny (ang. *logical disk*), jakkolwiek w szeregu programów te pojęcia bywają używane zamiennie bądź nieprawidłowo.

[185] Zob. np.: J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 31.; A. Kegel, Z. Kegel: *Przepisy*…, op. cit., s. 61–62.

[186] Sąd Najwyższy w wyroku z 10 maja 1982 r. (II KR 82/82) stwierdził m.in.: „Przepisy procedury karnej nie określają i nie mogą określać zakresu badań specjalistycznych wykonywanych przez biegłych, gdyż potrzeba przeprowadzenia stosownych badań i ich zakresu choć pozostaje pod kontrolą organu procesowego kierującego badaniem biegłych należy również do „wiadomości specjalnych".

W postanowieniu Izby Karnej Sądu Najwyższego z 25 czerwca 2003 r. (IV KK 8/03) sąd stwierdził: „w doborze metod i badań specjalistycznych biegły jest niezależny od organu procesowego, co nie oznacza, iż nie podlega jego kontroli".

[187] W wyroku z 7 lutego 1986 r. (IV KR 15/86) Sąd Najwyższy stwierdził: „Nie należy do kompetencji stron decydowanie, jakie metody badawcze dla stwierdzenia okoliczności mających istotny wpływ na rozstrzygnięcie sprawy okażą się przydatne w razie konieczności wykorzystania wiadomości specjalnych (…) strony mają prawo kontrolowania, czy wszystkie dostępne metody badawcze znane są biegłym i czy były wykorzystane. Jeśli biegli nie uznali za celowe posłużenie się niektórymi z nich, winni stanowisko swoje należycie uzasadnić. Uzasadnienie to podlega, jak każdy dowód, ocenie sądu".

Dość spektakularna kontrola sądowa znajomości metod badawczych przez biegłego miała miejsce w sprawie dotyczącej strat w PZU:

„Biegła Jadwiga Młynarczyk, która o kilkadziesiąt milionów pomyliła się w wyliczaniu strat w PZU Życie, po raz 18. występuje przed sądem. Sąd dopytuje, jaką metodą biegła określiła ryzyko inwestycyjne. Biegła zwleka z odpowiedzią. Wreszcie sędzia Krzysztof Petryna pyta wprost:

Sędzia: A metodę McKenziego pani zna?

Biegła: Tak.

Sędzia zdziwiony: Ale proszę pani, ja tę metodę wymyśliłem przed chwilą!". (Źródło: „Gazeta Wyborcza" z 8 maja 2004 r., http://www.archiwum.wyborcza.pl/Archiwum/

sze Andrzej Gaberle „sugestie w tym zakresie ze strony organu procesowego są zatem dopuszczalne, biegli zaś – jeśli nie uznają ich za trafne – powinni uzasadnić, dlaczego się do nich nie zastosowali, lecz nie są nimi związani"[188].

Tadeusz Widła[189] podaje cztery wskazania, którymi powinien kierować się biegły podczas wyboru metody. Są to:

- ✓ trafność metody;
- ✓ niezawodność metody[190];
- ✓ zasada ponoszenia kosztów rzeczywiście niezbędnych;
- ✓ popularność metody.

Z punktu widzenia biegłego informatyka na podkreślenie zasługuje możliwość wykorzystania w opiniowaniu zaleceń Polskich Norm oraz norm i standardów międzynarodowych (ISO[191], IEC[192], ITU-T[193], IEEE[194], dokumentów IETF[195] itp.). Należy pamiętać, że choć – zgodnie z art. 4 ust. 3 oraz art. 5 ust. 3 ustawy o normalizacji (dalej UON) stosowanie norm jest, co do zasady, dobrowolne – to dla biegłego, będącego przecież przedstawicielem nie własnych poglądów, ale dyscypliny wiedzy i techniki, stosowanie zarówno znormalizowanej nomenklatury jak i uwzględnianie opisanych w normach zasad i zaleceń jest podejściem rozsądnym. Oczywiście normy nie muszą za każdym razem wyznaczać jedynych, czy najlepszych standardów postępowania (choć oczywiście powinny do tego

1,0,4054232,20040508RP-DGW,JAK_BIEGLA_DO_TEGO_DOSZLA,.html). *Nota bene* „metoda McKenziego" jest nazwą metody fizjoterapeutycznej.

[188] A. Gaberle: *Dowody*…, op. cit., s. 181.

[189] Zob. J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 32 i nast.

[190] Powołany tekst wyjaśnia pojęcia trafności i niezawodności, odwołując się do częstości udanych identyfikacji, niezawodności interpresonalnej oraz intrapersonalnej. Posługując się nomenklaturą stosowaną do zagadnień pomiarowych należałoby mówić o dokładności, precyzji, powtarzalności i odtwarzalności, zaś w przypadku testów diagnostycznych (diagnostyka rozdzielcza) do czułości i swoistości testów.

[191] International Organization for Standardization (Międzynarodowa Organizacja Standaryzacyjna).

[192] International Electrotechnical Commission (Międzynarodowa Komisja Elektrotechniczna).

[193] International Telecommunication Union – Telecommunication Standardization Sector (Sektor Normalizacji Telekomunikacji Międzynarodowej Unii Telekomunikacyjnej).

[194] The Institute of Electrical and Electronics Engineers (Instytut Inżynierów Elektryków i Elektroników).

[195] Internet Engineering Task Force.

zmierzać); w konkretnych przypadkach działanie wbrew zapisom norm może być działaniem racjonalnym[196], niemniej wskazane jest odwoływanie się do nich w opinii przynajmniej jako do materiału referencyjnego.

W literaturze przedmiotu podkreśla się, że biegłego przy wyborze metody badawczej nie dotyczy zasada *in dubio pro reo*, stosowanie której jest właściwe dla organu procesowego. Ścisłe stosowanie się do niej przez biegłych powodowałoby konieczność wyboru tych spośród metod badawczych, które minimalizują ryzyko błędu II rodzaju (wniosków fałszywej klasyfikacji – ang. *false positive*), czyli np. stwierdzenia popełnienia czynu zabronionego, gdy w rzeczywistości nie był on popełniony[197], z drugiej jednak strony – opinia biegłego zawierająca zbyt daleko idące czy pochopnie wyciągnięte wnioski może nieść z sobą poważne konkretne skutki prawne, społeczne i etyczne, stąd też wspomnianą zasadę biegli powinni mieć na uwadze[198]. Biegły nie jest stroną w sporze sądowym ani nie może pełnić roli rzecznika żadnej ze stron, a zatem nie powinien tłumaczyć wątpliwości na niczyją korzyść lub niekorzyść, a jedynie poinformować organ procesowy, że takie wątpliwości występują i jaki jest ich charakter, w szczególności – jeśli to możliwe – podać odpowiednie statystyki charakteryzujące zastosowaną metodę badawczą (np. oszacowanie prawdopodobieństwa popełnienia błędów pierwszego i drugiego rodzaju, poziom istotności czy maksymalny błąd szacunku zastosowanych testów).

3.5 Opis czynności badawczych i ich wyników

Opinia biegłego nie może sprowadzać się do samych tylko wniosków. KPC formułuje to zalecenie w ten sposób, że powinna ona zawierać uzasadnienie[199], zaś KPK mówi o sprawozdaniu z przeprowadzonych czynności

[196] W szczególności, biorąc pod uwagę przewlekłość procesu normalizacyjnego, może się zdarzyć, że obowiązujące normy zawierają uregulowania przestarzałe z punktu widzenia rozwoju techniki i praktyk działania, stąd też – szczególnie w przypadku opiniowania w sprawach związanych z oceną należytej staranności wywiązywania się z umów (np. odnośnie do tworzenia oprogramowania, wdrażania systemów informatycznych, usług administracji itd.) – nie można ograniczyć się jedynie do samej konkluzji odnośnie do zgodności z normą.

[197] Zob. J. Wójcikiewicz: *Ekspertyza*…, op. cit., s. 32.

[198] Zob. np.: J. Kunz: *Błąd*... , op. cit.

[199] Art. 285 § 1 KPC: Opinia biegłego powinna zawierać uzasadnienie.

i spostrzeżeń oraz opartych na nich wnioskach[200]. Nie jest więc możliwe sprowadzenie opinii tylko do samych wniosków. Za co najmniej wątpliwą praktykę można uznać również wyciąganie wniosków tylko „na podstawie osobistej wiedzy i doświadczenia biegłego", która to formuła czasami bywa używana i nadużywana w opiniach biegłych[201]. W orzecznictwie istnieje

[200] Art. 200 § 2 KPK: Opinia powinna zawierać:
(…)
5) sprawozdanie z przeprowadzonych czynności i spostrzeżeń oraz oparte na nich wnioski.

[201] Z drugiej strony nie zawsze istnieje możliwość i sens znalezienia odpowiednich źródeł literaturowych, czy wyników badań, szczególnie, jeśli biegły miałby cytować własne opracowania, czy jeśli odpowiedzi na pytania zadawane przez uczestnika postępowania mieszczą się w kanonie nie wiadomości specjalnych ale ogólnych. Bocheński przytacza w swoich wspomnieniach następującą historię, kiedy został powołany jako biegły *ad hoc* przez sąd w Republice Południowej Afryki: „Ponad sto pięćdziesiąt osób, przeważnie czarnych, zostało oskarżonych o zdradę i postawionych przed sąd wyjątkowy na podstawie ustawy wyjątkowej. Główny zarzut stawiany im brzmiał, że są, względnie byli, komunistami, co według prawa południowoafrykańskiego było samo w sobie karalnym przestępstwem. Ponieważ jednak policja prowadząca proces (kraj nie posiadał prokuratury, policja najmowała po prostu adwokatów) nie bardzo rozumiała, czym komunizm właściwie jest, postanowiono sprowadzić sobie rzeczoznawcę (...). Nie namyślając, się wiele, zgodziłem się. (...). W Pretorii miałem bardzo dogodne warunki pracy. Policja skonfiskowała oskarżonym, którzy zresztą odpowiadali z wolnej stopy, dokumenty i książki i pozostawiła mi je do dyspozycji. Miałem wskutek tego wgląd w funkcjonowanie południowoafrykańskiej partii komunistycznej. Oto próbka mojej działalności. Referuję mój pogląd na jednego z oskarżonych. Moim zdaniem, ani śladu komunizmu. Na to jeden z adwokatów policji: przecież znaleziono u niego książkę rosyjską. Odpowiadam, że to prawda, ale książka jest Bierdiajewa, znanego antykomunisty. Na to oni, czy ja mogę to udowodnić. Przyznaję, że straciłem panowanie nad sobą, palnąłem pięścią w stół, mówiąc: »Gentleman dowód jest ten, że ja wam to mówię«(...). Trybunał wyjątkowy, mianowany specjalnie przez rząd do sądzenia sprawy na podstawie ustawy wyjątkowej, ostatecznie uwolnił wszystkich oskarżonych od winy i kary (...). Przed moim odlotem przyszedł do mnie członek ławy obrońców, prosząc, abym nie odjeżdżał, bo bał się, że beze mnie zrobią komunistów ze wszystkich oskarżonych. Pomylił się i przesadził mój wpływ na proces. Niemniej cieszę się, że mogłem w pewnej mierze przyczynić się do uwalniającego wyroku" (J. Bocheński: *Wspomnienia*, PHILED, Kraków 1994, s. 257). Oczywiście powołanie się w ten sposób na własne doświadczenie i wiedzę biegłego miało tu uzasadnienie, o tyle, że był on w tym czasie jednym z najwybitniejszych sowietologów na świecie, redaktorem i współautorem niemal tysiącstronicowego *Handbuch des Weltkommunisimus*, inicjatorem, dyrektorem i wykładowcą rządowego Ost-Kolleg w Kolonii.

szereg orzeczeń dotyczących konieczności zawarcia w opinii odpowiedniego uzasadnienia[202].

Dobrą praktyką jest zamieszczanie w opinii właściwie sporządzonej bibliografii oraz odsyłaczy do źródeł literaturowych; zachować natomiast należy ostrożność z cytowaniem fragmentów publikacji (może to budzić wątpliwości z punktu widzenia prawa autorskiego – opinia bowiem jest niewątpliwie dokumentem urzędowym w sensie art. 4 Prawa Autorskiego, w związku z czym zacytowany w niej fragment utworu staje się również fragmentem dokumentu urzędowego, co pozbawia go znamion utworu; w szczególności przytoczenie dzieła w całości mogłoby być równoważne z wywłaszczeniem autora z praw majątkowych do utworu, którym dzieło w ten sposób przestałoby być. Bezpieczniejszym wyjściem jest dołączenie kopii fragmentów odpowiedniego materiału źródłowego do opinii, co ma sens tylko wtedy, jeśli mowa o publikacjach niedostępnych w bibliotekach, księgarniach czy w Internecie, w pozostałych przypadkach wystarczy opis bibliograficzny).

Opis czynności badawczych powinien być na tyle szczegółowy, aby móc umożliwić ocenę metodologicznej poprawności ich wykonania, a więc np. przeprowadzając testy wydajnościowe aplikacji należy dokładnie opisać warunki badania, to jest m.in. przy użyciu jakiego oprogramowania przeprowadzono testy, jak było ono skonfigurowane, jakie były parametry testów obciążeniowych, jaka była konfiguracja i wydajność urządzeń (pamięci masowej, urządzeń sieciowych), czy na stanowisku badawczym były uruchomione inne procesy i jakie obciążenie one generowały, pod kontrolą jakiego systemu operacyjnego i w jakiej wersji prowadzono badania itd. Oczywiście oprócz opisu warunków badania należy podać jego wyniki oraz przeprowadzić ich dyskusję[203]. Pod tym względem zasady metodolo-

[202] Jako przykłady można podać następujące fragmenty wyroków:

- ✓ wyrok Sądu Najwyższego z 19 maja 1998 r. (II UKN 55/98): „Zgodnie z art. 285 KPC opinia biegłego powinna zawierać uzasadnienie, a więc stwierdzenia możliwe do sprawdzenia przez czytających tę opinię";
- ✓ wyrok Sądu Najwyższego z 29 lipca 1999 r. (II UKN 60/99): „Opinia biegłego powinna zawierać uzasadnienie sformułowane w sposób przystępny i zrozumiały także dla osób nieposiadających wiadomości specjalnych".

[203] W szczególności, jeśli otrzymane wyniki odbiegają od spodziewanych, należy rozpatrzeć możliwe przyczyny takiego stanu rzeczy. Może to być uzasadnienie dla przeprowadzenia kolejnych badań mających na celu wyeliminowanie ewentualnych błędów.

gicznie dokumentowania ekspertyzy nie różnią się od zasad opisu innych badań naukowych.

Od strony formalnej w postępowaniu karnym, zgodnie z art. 200 § 2 KPK, opinia powinna zawierać:

1) imię, nazwisko, stopień i tytuł naukowy, specjalność i stanowisko zawodowe biegłego;

2) imiona i nazwiska oraz pozostałe dane innych osób, które uczestniczyły w przeprowadzeniu ekspertyzy, ze wskazaniem czynności dokonanych przez każdą z nich;

3) w wypadku opinii instytucji – także pełną nazwę i siedzibę instytucji;

4) czas przeprowadzonych badań oraz datę wydania opinii;

5) sprawozdanie z przeprowadzonych czynności i spostrzeżeń oraz oparte na nich wnioski;

6) podpisy wszystkich biegłych, którzy uczestniczyli w wydaniu opinii.

KPC i KPA nie nakładają takich wymogów na zawartość opinii, niemniej wydaje się celowe zamieszczanie powyższych elementów również w postępowaniu w sprawach cywilnych i administracyjnych. Na uwagę zasługuje konieczność rozróżnienia osób uczestniczących w przeprowadzeniu ekspertyzy od biegłych wydających opinię (w szczególności uczestniczyć w przygotowaniu ekspertyzy mógł np. laborant niemający wpływu na późniejsze wnioskowanie biegłego)[204].

3.6 Formułowanie wniosków

Zgodnie z tym co napisano powyżej, jedną z najistotniejszych kwestii dotyczących formułowania wniosków z ekspertyzy jest konieczność w miarę możliwości dokładnego określenia stanowczości wniosków. Rozsądnym wyjściem wydaje się postulowane m.in. w pracy Wójcikiewicza[205] stopniowanie kategoryczności wniosków wg skali:

- ✓ pozytywne wnioski stanowcze, zwane też kategorycznymi;
- ✓ pozytywne wnioski uprawdopodabniające;

[204] Ma to konsekwencje dla ewentualnych późniejszych ról procesowych (art. 200 § 3 KPK: Osoby, które brały udział w wydaniu opinii, mogą być, w razie potrzeby, przesłuchiwane w charakterze biegłych, a osoby, które uczestniczyły tylko w badaniach – w charakterze świadków).

[205] J. Wójcikiewicz: *Ekspertyza*…, op. cit.

- ✓ pozytywne wnioski niewykluczające;
- ✓ wnioski nierozstrzygające;
- ✓ uprawdopodabniające wnioski negatywne;
- ✓ niewykluczające wnioski negatywne;
- ✓ stanowcze wnioski negatywne[206].

Propozycje tego rodzaju budzą jednak kontrowersje[207], co jest zresztą o tyle uzasadnione, że skala taka – aby była użyteczna – musiałaby być powszechnie stosowana i jednakowo interpretowana przez wszystkich biegłych (znormalizowana). Zdzisław Marek[208] proponuje inny sposób podziału opinii, mianowicie czterostopniową skalę obejmującą:

- ✓ opinie stanowcze;
- ✓ opinie o wysokim stopniu prawdopodobieństwa;
- ✓ opinie alternatywne;
- ✓ brak opinii z powodu niemożności zebrania wystarczających informacji.

Tego rodzaju podejście również może być jednak uznane za kontrowersyjne. Na przykład Piotr Kowalski i Janusz Długopolski krytykują posługiwanie się pojęciem „stopień prawdopodobieństwa"[209], zauważając, że

[206] Ibid., s. 36–37.

[207] Zob. np.: J. Widacki: *Recenzja książki J. Wójcikiewicza: Eskpertyza sądowa*, „Palestra" Nr 1 2/2003, dostępna na: http://palestra.pl/index.php?go=artykul&id=907.

[208] Zob. Z. Marek: *Wybrane…*, op. cit., s. 241.

[209] „Posługiwanie się pojęciem prawdopodobieństwo stanowi wyraźne odwołanie do pojęć matematycznych, a określenie stopień sugeruje istnienie jakiejś uporządkowanej powszechnie przyjętej skali, a tymczasem w przytłaczającej większości wydawanych opinii wyliczeń rachunku prawdopodobieństwa się nie stosuje, a także nie istnieje żadna skala stopniowania. Chcąc zatem pozostać w zgodzie z warsztatem metodologicznym biegłego, niezbędne jest zrezygnowanie z nic nieznaczącej słownej hybrydy, jaką jest określenie »stopień prawdopodobieństwa« na rzecz przyjęcia przez sąd »umotywowanej możliwości« zaistnienia określonego zdarzenia, wynikającej ze stanu faktycznego sprawy. Taka sytuacja jest wyraźnym sygnałem o wyczerpaniu możliwości biegłego na rzecz odwołania się do rozstrzygnięć natury czysto prawnej i to wyłącznie przez sąd, a nie przez biegłego.
Opiniując o związku przyczynowym, biegły może zawrzeć we wnioskach jedynie trzy następujące konkluzje: 1) przyjąć istnienie związku przyczynowego, 2) odrzucić jego występowanie oraz 3) stwierdzić brak możliwości przyjęcia albo odrzucenia związku przyczynowego na podstawie zebranego materiału dowodowego.
Przyjęcie przez sąd orzekający »umotywowanej możliwości« stanowić będzie rozwinięcie konkluzji biegłego, która nie przyjmuje i nie odrzuca związku przyczynowego, lecz jest

trudno stosować pojęcie prawdopodobieństwa bez odpowiednich matematycznych wyliczeń jego wartości. Z drugiej jednak strony w wielu zastosowaniach życiowych prowadzi się szacowanie prawdopodobieństwa nie w oparciu o ścisłe operacje matematyczne, ale metodą rangowania ocen eksperckich[210]. Oczywiście stwierdzenie, że coś jest (zaledwie) prawdopodobne nie jest dla sądu w wielu przypadkach wystarczające do wnioskowania o stanie faktycznym (np. do kategorycznego stwierdzenia adekwatnego związku przyczynowo-skutkowego). Z drugiej jednak strony tego rodzaju informacja może być użyteczna dla sądu w innych sprawach (np. związanych z zachowaniem należytej staranności przy zabezpieczaniu się przed jakimiś – zaledwie przecież prawdopodobnymi – zagrożeniami) czy w połączeniu z innymi dowodami, którymi przecież zazwyczaj sąd dysponuje. Gdyby zresztą wykluczyć możliwość wydawania opinii innych niż stanowcze, mogłoby się okazać, że w większości przypadków opinii nie da się wydać. Rozważania takie mogą wydawać się z jednej strony oczywiste, a z drugiej – dość abstrakcyjne, mogą mieć one bardzo konkretne – a cza-

stwierdzeniem, iż stan faktyczny sprawy nie upoważnia biegłego do wydania stanowczej opinii. Sąd zaś winien na podstawie całokształtu zebranego w sprawie materiału dowodowego oraz zasady swobodnej oceny dowodów orzec, że możliwe jest przyjęcie istnienia związku przyczynowego nie w oparciu o twierdzenia biegłego o prawdopodobieństwie, lecz stwierdzonej przez sąd możliwości zaistnienia określonego stanu zdarzeń". P. Kowalski, J. Długopolski: *Kategoryczność opinii biegłego sądowego medyka w sprawach cywilnych*, „Palestra" Nr 9–10/2, http://www.palestra.pl/index.php?go=artykul&id=2808.

[210] Tego rodzaju oszacowania prawdopodobieństwa stosuje się np. przy analizach ryzyka biznesowego. Przewodnik [PKN ISO Guide 73:2009], w definicji 3.6.1.1 (definicja z [ISO 31000:2009 – 2.19]) rozróżnia prawdopodobieństwo rozumiane matematycznie (*probability*) i potocznie (*likelihood*):

„Likelihood chance of something happening

NOTE 1: In risk management terminology, the word »likelihood« is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

NOTE 2: The English term »likelihood« does not have a direct equivalent in some languages; instead, the equivalent of the term »probability« is often used. However, in English, »probability« is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, »likelihood« is used with the intent that it should have the same broad interpretation as the term »probability« has in many languages other than English" [ISO 31000:2009– 2.19], [ISO Guide 73:2009 – 3.6.1.1].

sami również wymagające dłuższego zastanowienia – zastosowania[211]. Jak zatem widać, obie konstrukcje (określenie stopnia stanowczości wniosków

[211] W literaturze przedmiotu powtarzana jest przestroga, że „najbardziej niebezpieczne jest stwierdzenie (...) NIE MAM ŻADNEGO DOWODU, ABY TO STWIERDZIĆ, LECZ NIE MOŻNA TEGO WYKLUCZYĆ (Z. Marek: *Wybrane*…, op. cit., s. 242, podkr. w oryginale). W cytowanej pracy przytoczony jest przypadek, w którym na podstawie zdania biegłego: „Co prawda nie znaleziono żadnych śladów krwi w pewnej odległości od zwłok, ale nie można wykluczyć obecności takich śladów, chociaż ich nie stwierdzono" oskarżono o sfałszowanie opinii innego biegłego, który – prawidłowo – na pytanie prokuratora odpowiedział: „wobec faktu nieznalezienia żadnych śladów krwi biegły nie ma podstawy do snucia jakichkolwiek wniosków" (ibid., s. 114). Por. także np. P. Kowalski, J. Składzień: *Opiniowanie w sprawach cywilnych i karnych jako problem w praktyce biegłego*, „Otorynolaryngologia" Nr 3(3)/2004).
Z własnej praktyki autora niniejszej monografii można przytoczyć pytanie skierowane przez adwokata jednej ze stron procesu cywilnego do biegłego: „Czy działania pracownika pozwanego przyczyniły się do ułatwienia ataku hackera na system informatyczny?". Sprawa dotyczyła odszkodowania za naruszenie zasad bezpieczeństwa, jakie zdaniem powoda winien był zapłacić pozwany (instytucja finansowa). Atakujący, podszywając się pod powoda, wyłudził z konta jego firmy znaczną sumę. Pracownik pozwanego (osoba obsługująca oprogramowanie służące do zlecania przelewów) niewątpliwie naruszył kilka zasad bezpieczeństwa i to tak, że dzięki temu możliwe byłoby przełamanie jednego z zabezpieczeń, niemniej same w sobie te działania nie wystarczyłyby włamywaczowi do skutecznego ataku, bowiem informacja chroniona była jeszcze innymi zabezpieczeniami. Z drugiej strony inne osoby mające styczność z systemem informatycznym powoda (w tym jego administrator) również nie przestrzegały zasad bezpieczeństwa, co w konsekwencji umożliwiło atakującemu skuteczny atak. W pozwie powód powoływał się na zasadę odpowiedzialności kontraktowej (pozwany nie wywiązał się z obowiązku zachowania zasad bezpieczeństwa), ale jeśli odpowiedź biegłego byłaby twierdząca w grę wchodziłaby nawet odpowiedzialność na zasadzie winy. W rzeczywistości – niemożliwe było ustalenie czy zabezpieczenie, o którym mowa, atakujący przełamał dzięki niefrasobliwości pracownika pozwanej instytucji czy też innych osób (w tym pracowników powoda). Żeby uniknąć wspomnianego zdania („Nie mam żadnego dowodu, aby to stwierdzić, lecz nie można tego wykluczyć") powód powinien raczej pytać biegłego po pierwsze o to, czy zachowanie pozwanego stanowiło naruszenie zasad bezpieczeństwa (odpowiedź: „tak"), a po wtóre o to, czy w tym przypadku istniał związek przyczynowo-skutkowy pomiędzy tym konkretnym naruszeniem a włamaniem (odpowiedź: „nie ma podstaw do snucia jakichkolwiek wniosków"). Na pytanie postawione jak w oryginale biegły powinien zatem odpowiedzieć „nie ma podstaw do snucia jakichkolwiek wniosków", natomiast na pytanie „Czy działania powoda mogły przyczynić się do ułatwienia ataku hackera na system informatyczny?" – „tak". Oczywiście w tej sytuacji trudno było spodziewać się satysfakcjonującego dla powoda wyroku i rzeczywiście powództwo zostało oddalone w pierwszej instancji, a sąd II instancji wyrok podtrzymał.

oraz posługiwanie się pojęciem „umotywowanej możliwości") są w literaturze krytykowane. Zdaniem autora niniejszej monografii zdecydowanie lepszym wyjściem jest posługiwanie się pierwszą z nich, oczywiście z zaznaczeniem, że użycie liczbowych wartości prawdopodobieństwa jest możliwe tylko w przypadku zastosowania odpowiednich obliczeń statystycznych. W przeciwnych przypadkach należy posługiwać się tradycyjnymi sformułowaniami opisowymi („istnieje pewne prawdopodobieństwo", „z prawdopodobieństwem bliskim pewności", „niezwykle mało prawdopodobne jest, że"), przy czym rozważań tych nie można opierać na braku przesłanek[212].

Konieczne jest również czytelne i metodologicznie poprawne uzasadnienie zarówno wniosku, jak i wybranej metody badawczej. W szczególności o ile w normalnej działalności informatyk-administrator czy serwisant nie spotyka się raczej z próbami celowego wprowadzenia go w błąd, o tyle w przypadku sporu sądowego (a już szczególnie procesów karnych), nie można opierać swojego rozumowania wyłącznie w oparciu o informacje uzyskane od osób trzecich (zeznań stron i świadków, czy dokumentów przedstawionych przez strony), bez ich starannego sprawdzenia[213], które

Podobne wątpliwości może budzić użycie słów „ten" i „taki" (w odniesieniu do tego – a więc ściśle określonego, konkretnego – zdarzenia i skutku takiego [jak] – a więc podobnego, potencjalnego).

[212] Należy odróżnić brak przesłanek od braku śladów. Brak śladów (w stosunkowo rzadkich przypadkach) może być podstawą do wyciągania wniosków, zgodnie z sylogizmem *modus tollendo tollens*: $[(p \rightarrow q) \wedge \neg q] \Longrightarrow \neg p$. Tadeusz Kotarbiński (*Elementy teorii poznania, logiki formalnej i metodologii nauk*, Warszawa, PWN 1986, s. 148), podaje przykład: „Jeżeli nie ma śladów uderzeń na zwłokach, a przy tym gdyby zmarły był bity przed śmiercią, to by były ślady uderzeń na zwłokach, tedy nieprawda, że zmarły był bity przed śmiercią", co może nie jest do końca idealnym przykładem, ale dobrze oddaje zasadę tego sylogizmu. Warto pamiętać, że aby takie rozumowanie było sprawne, przesłanka większa sylogizmu musi być spełniona – wynikanie musi rzeczywiście zachodzić. W przypadku opinii informatycznych brak – na przykład – w logach systemowych zapisów wskazujących na włamanie do systemu może świadczyć zarówno o tym, że włamania nie było, jak i o tym, że włamywacz przejąwszy kontrolę nad systemem usunął odpowiednie zapisy z logów (nie jest prawdziwe zdanie, że „jeśli było włamanie, to muszą być odpowiednie zapisy w logach" – przesłanka większa sylogizmu nie jest spełniona).

[213] Widać tu pewną analogię do problemów, przed którymi stoją medycy sądowi: o ile bowiem dla lekarza klinicysty wywiad z pacjentem jest jednym z podstawowych źródeł wiedzy, o tyle np. medyk sądowy musi spodziewać się, że pacjent, nawet nieświadomie, będzie

zresztą jest nie zawsze możliwe. Warto przypomnieć w tym miejscu ponownie (por. rozdział 2.3.4), że wykonywanie samodzielnych oględzin badanych systemów czy toczenie nieformalnych rozmów ze świadkami i przedstawicielami stron nie są narzędziami badawczymi informatyki i jako takie nie powinny być przez biegłego nigdy podejmowane oraz że do roli biegłego nie należy ocena prawdziwości i wartości merytorycznej zeznań czy dokumentów (ta bowiem zarezerwowana jest dla organu procesowego, zgodnie z zasadą swobodnej oceny materiału dowodowego). Jeśli rozumowanie biegłego oparte jest na zeznaniach świadka (w szczególności zaś, jeśli w materiale procesowym istnieją dowody zaprzeczające tym zeznaniom, np. zeznania innego świadka) konieczne jest dokładne opisanie zaistniałej sytuacji, zaś – jeśli to konieczne – należy formułować opinie alternatywne[214] („jeśli prawdziwe są zeznania świadka A to…, jeśli natomiast prawdziwe są zeznania świadka B, pozostające z nimi w sprzeczności to…"). Przy formułowaniu i rozumieniu opinii biegłego mogą pojawić się również problemy językowe. Język informatyki odbierany bywa przez prawników jako trudny i wysoce hermetyczny (podobnie jak język prawników jest odbierany przez informatyków), z tego też względu należy bardzo dbać o precyzję i kompletność wypowiedzi[215] oraz o jej komunikatywność[216]. Przede wszystkim należy

starał się przedstawić swój (subiektywnie postrzegany jako zły) stan zdrowia jako skutek błędów lekarza, z którym znajduje się w sporze. Podobnie np. pracownicy instytucji niezadowoleni z usług firmy outsourcingowej administrującej jej systemem informatycznym będą skłonni do przedstawiania wszystkich nieprawidłowości i problemów związanych z eksploatacją tego systemu jako skutków błędów administratora.

[214] Opinie alternatywne (tj. zawierające wnioski alternatywne) nie naruszając zasady swobodnej oceny materiału dowodowego przez organ procesowy pozwalają mu uzyskać wiedzę na temat konsekwencji, jakie niesie za sobą uznanie za prawdziwą wyeksplikowanej przez uczestnika postępowania tezy bądź jej zaprzeczenia.

[215] W mowie potocznej informatycy mają skłonność do posługiwania się stwierdzeniami kategorycznymi, nawet w przypadkach, kiedy nie jest to do końca uprawnione. Dodatkowo pewne sformułowania, nawet poprawne z informatycznego punktu widzenia, mogą być niezrozumiałe dla laika. Stwierdzenie: „wystąpił błąd w programie" prawnik będzie raczej skłonny uznać za równoważną stwierdzeniu, że w programie tkwił błąd, który właśnie się ujawnił, w czasie kiedy dla informatyka oczywiste jest, że miejsce ujawnienia się skutków błędu może być stosunkowo odległe od miejsca jego wystąpienia, a nieoczekiwane działanie programu komputerowego może wynikać zarówno z błędu w jego kodzie, jak i z błędnych działań użytkownika, błędów w systemie operacyjnym, problemów z współpracą z innym programem, niewłaściwych danych wprowadzonych do przetwarzania, a nawet z błędów

posługiwać się fachowym (a nie pseudo-fachowym) językiem. Dla informatyka będzie to przede wszystkim język Polskich Norm. Stanowczo należy zrezygnować ze zwyczaju dołączania do opinii tworzonych *ad hoc* słowniczków (z dużym prawdopodobieństwem tworząc samodzielnie definicje biegły popełni gdzieś błąd, nie uwzględni jakichś przypadków szczególnych, a w przypadku powołania kolejnych biegłych narazi ich na dodatkową pracę, a siebie na niepotrzebną krytykę przed sądem).

Wątpliwą wartość ma metoda fabularyzowania wypowiedzi biegłego przez stosowanie różnego rodzaju uproszczeń czy rozbudowanych paraleli, mających za zadanie wyjaśnić sądowi sposób działania poszczególnych mechanizmów technicznych. Istnieje duże ryzyko, że osoby pozbawione wiedzy fachowej źle zinterpretują tego rodzaju przypowieści zwracając raczej uwagę na akcydentalne szczegóły niż na ich zamierzone przesłanie. Oczywiście można czasem stosować porównania i analogie tam, gdzie mają one proste przełożenie na znaną sądowi rzeczywistość „nieinformatyczną" (np. nie będzie przesadą wyjaśnienie mechanizmów zapewniania w protokołach sieciowych kontroli niezawodności transmisji[217] metodą potwierdzeń[218] przez odwołanie się do przykładu zwrotnego potwierdzenia odbioru wykorzystywanego w tradycyjnych usługach pocztowych), należy jednak tego rodzaju środków używać z umiarem. Rzeczą oczywistą jest

sprzętowych. Nawet więc jeśli program zakończy swoją pracę informacją o błędzie krytycznym nie oznacza to jeszcze, że przyczyną jego zaistnienia był błąd programisty, czy tym bardziej, że twórca programu źle wypełnił zadanie postawione przez osobę, która jego napisanie zleciła. Błąd, który ujawnił się w czasie wykonywania jakiegoś programu (a nawet w jego przestrzeni adresowej) może znajdować się (mógł być popełniony) zupełnie poza programem, w którym się ujawnił.

[216] W pracy Kunza: *Błąd…*, op. cit., s. 9, zacytowany jest, przedstawiony pierwotnie przez D.M. Paula na łamach czasopisma „Medicine and law" swoisty „dekalog biegłego" dla medyków sądowych zawierający m.in. ostrzeżenia: „Nie patrz z góry na prawników, nie są głupcami. Uważaj, bo o medycynie słyszeli od mądrzejszych od Ciebie", „Nie używaj słownictwa medycznego, staraj się mówić językiem codziennym" itd. W przypadku informatyki jednakże posługiwanie się językiem potocznym może być ryzykowne. Z dwojga złego lepsza jest wypowiedź jednoznaczna, a trudna do zrozumienia (sąd może dopytać biegłego, jak ją zrozumieć), niż wypowiedź przekazana prostym językiem, ale możliwa do zrozumienia na wiele sposobów (istnieje ryzyko, że sąd rozumie ją niewłaściwie, ale będzie przekonany, że zrozumiał ją prawidłowo).

[217] Ang. *reliable*.

[218] Ang. *acknowledgements*.

również to, że biegły powinien zarówno swoim zachowaniem, jak i językiem stosowanym w opinii czynić zadość wymaganiom kultury osobistej[219].

Z technicznego punktu widzenia istnieją dwa podejścia do umieszczania wniosków: na początku bądź na końcu opinii. Pierwsze z nich sprawia, że decydent procesowy szybko i łatwo uzyskuje informacje o konkluzji opinii, niestety powoduje czasem, że na lekturze konkluzji kończy zapoznawanie się z opinią[220], co oczywiście samo w sobie jest naganne, mogą się bowiem zdarzyć – i zdarzają się – choćby np. omyłki pisarskie, prowadzące do zmiany sensu zdania, zarówno w sformułowanych przez biegłego wnioskach, jak również w sformułowanym przez organ procesowy zakresie i przedmiocie opinii, wskutek czego opinia wprawdzie prawidłowo odpowiada na pytania, ale nie te pytania, które zadający zamierzał zadać[221].

[219] Nie bez powodu jednak musiał tą kwestią zająć się Sąd Najwyższy, który w wyroku z 14 lutego 2013 r. (II CSK 371/12) stwierdził m.in.: „biegły sądowy nie powinien w tekście opinii zamieszczać uwag niemerytorycznych ani wyrażać swych ocen w nieodpowiedniej formie. Jest on powoływany przez sąd ze względu na swą wiedzę specjalną w danej dziedzinie potrzebną do rozstrzygnięcia sprawy, a takie uwagi i oceny zawsze obniżają wartość opinii biegłego oraz godzą w powagę wymiaru sprawiedliwości".
Sprawa dotyczyła opinii biegłego, który zawarł w niej sformułowania takie jak: „pieniactwo strony pozwanej", „nie jest zadaniem biegłego edukowanie pełnomocnika procesowego, który wręcz bzdury wypisuje", „czy jest to bezmyślność pełnomocnika strony pozwanej, czy brak kontroli nad tym, co się pisze w pismach procesowych".

[220] Zob. np.: M. Żołna: *Kryteria oceny opinii biegłych*, „Problemy Kryminalistyki" Nr 259/2008, s. 44–48.

[221] Skrajny chyba przypadek tego rodzaju (dopisanie słowa „nie" do konkluzji opinii) opisany jest w artykule *Przestępcy specjalnej troski* (A. Suworow, W. Krasucki, „Przegląd" Nr 36/2002, http://www.przeglad-tygodnik.pl/pl/artykul/przestepcy-specjalnej-troski-0): „Opinię wydało dwóch biegłych psychiatrów. Jednym z nich był lekarz z Nowej Soli, który udzielał prywatnych konsultacji podejrzanemu.
»Nie jest chory psychicznie«, konkludowali lekarze w pierwszym punkcie opinii.
– Stwierdziliśmy jedynie lekki niedorozwój umysłowy – przyznaje Eleonora Pillmann, psychiatra ze wskazaniem na to, że nie powinien odpowiadać za przestępstwo, które popełnił. Mógł jednak stawać przed sądem i składać zeznania w swojej sprawie.
Tak się jednak nie stało. Na opinii wydanej przez psychiatrów odręcznie dopisano słowo »nie«, wskazując na »błąd maszynistki«. W efekcie naniesionej poprawki pkt 5 brzmiał: »Nie może stawać przed sądem i składać zeznań w swojej sprawie«.
Pod odręcznymi zapiskami na dokumencie widnieją pieczęć i podpis prokuratora prowadzącego.

3.7 Ocena opinii biegłego, metaopinia, konfrontacja biegłych

Opinia biegłego, jak każdy dowód, podlega ocenie przez organ procesowy, zgodnie z zasadą swobodnej oceny dowodów. Z zagadnieniem tym związane są kwestie: rozróżnienia pomiędzy swobodną a dowolną oceną dowodów oraz wyjaśnienia ustawowych pojęć opinii niepełnej i niejasnej[222], z konsekwencjami negatywnej oceny opinii, bądź zaistnienia sprzeczności pomiędzy opiniami, związane są natomiast zagadnienia metaopinii (superekspertyzy) oraz konfrontacji biegłych.

Swobodna oceny dowodów jest w literaturze przeciwstawiana – znanej z prawa amerykańskiego – formalnej ocenie dowodów[223]. Zasada swobodnej oceny dowodów oznacza, że sąd samodzielnie decyduje o tym, które dowody uznać za wiarygodne; nie istnieją bowiem przepisy regulujące tryb oceny dowodów, ani ich hierarchia ważności. Ocena swobodna jednak to taka ocena, której słuszność można uzasadnić konkretnymi okolicznościami faktycznymi, wynikającymi z analizy innych przeprowadzonych

– Skontaktowałem się z biegłym, który sporządzał opinię zapewnia prokurator. Potwierdził błąd w trakcie przepisywania.
– Nie ma mowy o jakiejkolwiek pomyłce, czy błędzie maszynistki – ripostuje doktor Pillmann.
– To ja przepisywałam opinię. Badany przez nas mężczyzna mógł zeznawać".

[222] ***Art. 201 KPK**: Jeżeli opinia jest niepełna lub niejasna albo gdy zachodzi sprzeczność w samej opinii lub między różnymi opiniami w tej samej sprawie, można wezwać ponownie tych samych biegłych lub powołać innych.*
***Art. 285 § 3 KPC**: Jeżeli biegły nie może na razie udzielić wyczerpującej opinii, sąd wyznaczy termin dodatkowy do jej przedstawienia.*
***Art. 286 KPC**: Są może zażądać ustnego wyjaśnienia opinii złożonej na piśmie, może też w razie potrzeby zażądać dodatkowej opinii od tych samych lub innych biegłych.*
Art. 290 KPC
§ 1. Sąd może zażądać opinii odpowiedniego instytutu naukowego lub naukowo-badawczego. Sąd może zażądać od instytutu dodatkowych wyjaśnień bądź pisemnych, bądź ustnych przez wyznaczoną do tego osobę, może też zarządzić złożenie dodatkowej opinii przez ten sam lub inny instytut.

[223] Można spotkać się z tezą, że formalna ocena dowodów prowadzi do ustalenia „prawdy formalnej" (tutaj: wynikającej z przeprowadzenia dowodów zgodnie z ustaloną procedurą), podczas gdy ocena swobodna sprzyja ustaleniu prawdy materialnej. Rzeczywiście z formalną oceną dowodów związane są szczególnie bulwersujące przypadki uniewinnienia osób, które ewidentnie popełniły czyny karalne, ale dowody na popełnienie ich zostały zdobyte z naruszeniem zasad prawa. Zasada swobodnej oceny dowodów nie oznacza jednak nieistnienia zakazów dowodowych. Również w polskim orzecznictwie znane są wyroki uniewinniające zapadłe z powodu uzyskania dowodów z naruszeniem prawa.

dowodów, uwzględniająca kryteria obiektywne: zasady logicznego rozumowania, wiedzę, doświadczenie życiowe i zawodowe sędziego. Co więcej – sąd musi podać i wyjaśnić (w uzasadnieniu wyroku), dlaczego zdecydował się uznać za prawdziwe jedne dowody, a inne odrzucić. Jeśli ocena dowodów (w tym opinii biegłego) nie spełnia tych przesłanek, mówi się o ocenie dowolnej, która jest niedopuszczalna i może być podniesiona jako zarzut w apelacji bądź zażaleniu.

Odnośnie do pojęć niepełności i niejasności opinii wypowiedział się Sąd Najwyższy w wyroku z 7 października 2009 r. KK: „Opinia jest »niepełna«, jeżeli nie udziela odpowiedzi na wszystkie postawione biegłemu pytania, na które zgodnie z zakresem wiadomości specjalistycznych i udostępnionych mu materiałów dowodowych może oraz powinien udzielić odpowiedzi, lub jeżeli nie uwzględnia wszystkich istotnych dla rozstrzygnięcia konkretnej kwestii okoliczności albo też nie zawiera uzasadnienia wyrażonych w niej ocen i poglądów. Natomiast opinia »niejasna« to taka, której sformułowanie nie pozwala na zrozumienie wyrażonych w niej ocen i poglądów, a także sposobu dochodzenia do nich, lub też zawierająca wewnętrzne sprzeczności, posługująca się nielogicznymi argumentami".

W sytuacjach zaistnienia wątpliwości co do treści opinii, sąd zazwyczaj wzywa biegłego na rozprawę w celu ich wyjaśnienia, bądź też zleca wydanie opinii uzupełniającej temu samemu lub innemu biegłemu. W przypadku opinii informatycznych dość często spotykaną sytuacją jest uzupełnianie pytań przez organ procesowy (wnioski o wydanie kolejnych opinii) nie na skutek niepełności czy niejasności opinii, ale w wyniku zapoznania się organu z opinią i powzięcia kolejnych pytań wymagających odpowiedzi. Taki „iteracyjny" tryb pracy biegłego jest niekiedy nawet wskazany, często bowiem nie da się rozsądnie zadać pytań nie znając wyników jakichś (początkowych) badań. Natomiast rezygnacja z usług jednego biegłego i powołanie innego do udzielenia odpowiedzi na te same pytania może świadczyć o negatywnej ocenie opinii przez organ procesowy[224].

[224] W opisywanych w tej monografii dwóch przypadkach: malarza oskarżonego o wytwarzanie pornografii dziecięcej (zob. rozdział 5.1) oraz osoby oskarżonej o czyn z artykułu 267 § 1 KK przy okazji prowadzenia ataku SQL-injection (zob. rozdział 4.3) sąd, po zapoznaniu się z opinią biegłego (w pierwszym przypadku seksuologa, a w drugim – informatyka) zdecydował się na powołanie kolejnych biegłych, wnioski z opinii których były sprzeczne

Warto przy okazji zwrócić uwagę, że przedwczesne uznanie przez sąd opinii za niepełną czy niejasną może stać się przyczyną późniejszych problemów, może bowiem okazać się, że kolejna opinia jest dla sądu jeszcze trudniejsza do przyjęcia, a opinia pierwotna została zdyskredytowana niesłusznie[225], co skutkuje niemożliwością jej wykorzystania. Można wymienić kilka przykładowych sytuacji[226], które nie skutkują powstaniem możliwości automatycznego uznania opinii za niepełną czy niejasną:

- ✓ nie jest opinią niepełną opinia, w której biegli mający dostęp do całości akt sprawy, a niemający polecenia odniesienia się do konkretnych zawartych w nich materiałów, uzasadniają swoją opinię odwołując się do dokumentów w tych aktach zawartych, pomijając zeznania świadków[227];

---

z wnioskami biegłych powołanych pierwotnie i na których to wnioskach sąd ostatecznie się oparł.

[225] Por. np. wyrok Sądu Apelacyjnego we Wrocławiu z 5 września 2012 r. (II AKa 155/12): „Sposób procedowania jest trudny do zaakceptowania. Jeżeli sąd ocenił, iż opinia biegłego (…) jest niepełna lub niejasna winien sformułować pytania pod adresem biegłego i zakreślić czas biegłemu do udzielenia odpowiedzi na dodatkowe pytania".

[226] W zasadzie wiedza taka potrzebna jest bardziej sędziom niż biegłym, jakkolwiek z negatywną oceną opinii wiąże się zazwyczaj również obniżenie wynagrodzenia biegłego, a więc również z punktu widzenia biegłego warto wiedzieć, jakie mogą być przesłanki ewentualnego zażalenia na postanowienie dotyczące oceny wykonanej opinii i wynagrodzenia za nią.

[227] W postanowieniu Sądu Apelacyjnego we Wrocławiu z 19 stycznia 2012 r. (II A Kz 23/12, niepubl., wytłuszczenia w oryginale), sąd stwierdził m.in.: „W pierwszym z wysłowionych w treści zaskarżonego postanowienia zastrzeżeniu o znaczeniu istotnym, Sąd stwierdza, że biegli pominęli »źródła dowodowe jakim były zeznania świadków«. Tak sformułowane zastrzeżenie rodzić może pytanie, czego dotyczyło zlecenie Sądu kierowane pod adresem biegłych – wydania opinii tylko w kwestiach wymagających wiedzy specjalnej, czy też wydania **za sąd** swoistego orzeczenia w kwestii rozstrzygnięcia o zarzutach oskarżenia. W żadnym wypadku zadanie biegłych nie może polegać na kompleksowej analizie wszelkich zgromadzonych dowodów, w tym dowodów osobowych, dokonywania ich analizy i formułowania opinii w oparciu o własną ocenę ich treści i – co najważniejsze – wiarygodności. **Ocena dowodów, w tym ocena zeznań i wyjaśnień, stanowi wyłączną domenę sądu orzekającego**. Nie oznacza to naturalnie, że dowody osobowe nie mogą być źródłem informacji ważnych dla badań biegłego, zależnie od okoliczności danej sprawy i rodzaju ekspertyzy. Jeśli jednak staje się to konieczne, to nie biegły ma decydować na których ma opierać się dowodowych osobowych, lecz wskazać je powinien Sąd zlecający ekspertyzę. Teoretycznie można sobie wyobrazić sytuację, w której biegły wykorzystuje zeznania i wyjaśnienia jako źródła informacji, które następnie uwzględnia w trakcie badań i opiniowania, ale w takim wypadku spełnione zostać co najmniej dwa warunki *sine qua non*: a) uprawnienie

✓ brak odpowiedzi na pytanie sądu nie musi oznaczać, że opinia jest niepełna. Mogą zaistnieć sytuacje, w których na pytanie nie da się odpowiedzieć z przyczyn obiektywnych[228];

✓ niejasność opinii dla konkretnych sędziów nie oznacza jej obiektywnej niejasności[229], jeśli sąd nie powołuje innego biegłego, to

ich wykorzystania wynikać musi wprost z postanowienia Sądu, b) biegły musi wskazać na których zeznaniach opiera swoje własne ustalenia i w każdym wypadku, w którym w aktach sprawy znajdują wzajemnie sprzeczne dowody osobowe (w relacjach pomiędzy zeznaniami lub w relacjach pomiędzy zeznaniami, a wyjaśnieniami albo też, gdy zachodzi sprzeczność wewnętrzna w treści dowodu osobowego) musi formułować wnioski wariantowe. Uznanie zaś przez sąd tego lub innego wariantu za słuszny będzie zależna od tego, którym z wykorzystanych przez biegłego dowodów Sąd orzekający da wiarę)".

[228] W postanowieniu Sądu Apelacyjnego we Wrocławiu z 19 stycznia 2012 r. (II A Kz 23/12, niepubl.) sąd stwierdził: „(…) brak odpowiedzi na pytanie Sądu zlecającego ekspertyzę nie oznacza automatycznie, że opinia jest niepełna, jeżeli przyczyna braku odpowiedzi lub jej ograniczonego zakresu została racjonalnie i przekonywująco wyjaśniona przez biegłego. W konkretnych przypadkach niemożliwość udzielenia odpowiedzi na pytanie sądu, nie wyklucza wartości poznawczej opinii i w niczym nie obciąża biegłego. Żądanie zaś odpowiedzi wbrew wiedzy biegłego i wbrew okolicznościom uniemożliwiającym jej udzielenie, jest po prostu niedopuszczalne".

[229] W powołanym postanowieniu Sądu Apelacyjnego we Wrocławiu z 19 stycznia 2012 r. (II A Kz 23/12, niepubl., wytłuszczenia w oryginale) sąd stwierdził również „(…) niejasność opinii w odbiorze konkretnych sędziów (choć jest to kwestia zasadnicza) nie oznacza jeszcze obiektywnej niejasności lub niezrozumiałości opinii w ocenie innych uczestników postępowania, którzy także nie dysponują wiedzą ekspertalną. Ta sytuacja nie uszła uwadze ustawodawcy, który w art. 201 KPK stanowi, że »jeżeli opinia jest niepełna lub niejasna (…) można ponownie wezwać tych samych biegłych lub powołać innych«. Ustawa nakłada zatem nie obowiązek lecz uprawnienie powołania tych samych biegłych celem uzupełnienia opinii lub jej wyjaśnienia. Jest to bez wątpienia słuszne rozwiązanie, bowiem wskazuje na możliwość podjęcia alternatywnej decyzji co do powołania tych samych biegłych lub powołania innych. Ale przecież istnienie takiej ustawowej możliwości nie zwalnia sądu od uprzedniego podjęcia decyzji co do wiarygodności opinii. Nie sposób naturalnie uznać za wiarygodną opinię niejasną, co do trafności której sąd nie ma zatem pewności. Poprawna wykładnia art. 201 KPK nie pozostawia wszakże sądowi swobody decyzji. Jeśli sąd nie powołuje innego biegłego (…), to w takiej sytuacji ma w istocie rzeczy **powinność** powołania tych samych biegłych i zobowiązania ich do usunięcia wad opinii lub też do wyjaśnienia kwestii rodzących wątpliwości sądu. **W takim wypadku biegły ma obowiązek spełnienia żądania sądu**. Dopiero wtedy, gdy biegły odmówi spełniania tego obowiązku lub obowiązkowi temu nie sprosta i nie potrafi wytłumaczyć sądowi swoich racji oraz przekonać do ich słuszności, opinia biegłego może zostać uznana (…) za wadliwą".

powinien powołać tego samego biegłego i zobowiązać go do wyjaśnienia kwestii budzących wątpliwości;

- ✓ sąd w postępowaniu karnym nie ma możliwości arbitralnego zdyskwalifikowania opinii biegłego bez wykazania, że jest ona niepełna lub niejasna albo została sporządzona w sposób nierzetelny lub niekompletny[230].

Niezależnie od przyczyny, na skutek różnych okoliczności mogą w sprawie pojawić się sprzeczne opinie[231], co tworzy dla organu procesowego sytuację trudną, zazwyczaj bowiem nie jest on w stanie ocenić merytorycznej poprawności opinii, nie dysponując zwykle wiadomościami specjalnymi z dziedziny, której opinia dotyczy[232], nie powinien zresztą z opinią

[230] Sąd Najwyższy w wyroku z 3 października 2003 r. (V KK 50/03) stwierdził: „art. 201 KPK obliguje organ procesowy nie tylko do kontroli dowodu z opinii biegłych, ale również do wyjaśnienia ewentualnych wątpliwości i zastrzeżeń. Całkowita dyskwalifikacja opinii biegłych wymaga od sądu uprzedniego wykazania, że były one oparte na błędnych przesłankach, względnie, że nie odpowiadają aktualnemu stanowi wiedzy w danej dziedzinie lub też, że są sprzeczne z zasadami logicznego rozumowania. Procedura karna nie daje organowi procesowemu prawa do jednostronnego arbitralnego zdyskwalifikowania opinii biegłego bez wykazania, że jest ona niepełna lub niejasna albo została sporządzona w sposób nierzetelny lub niekompletny. W takich sytuacjach, sąd powinien w ramach obowiązku prawidłowego wyjaśnienia okoliczności będących przedmiotem dowodu podjąć próbę uzupełnienia dotychczasowej opinii, przez działanie przewidziane w art. 201 KPK".

[231] Jak wspomniano wcześniej, zdarzają się sytuacje powoływania nadmiarowej – wręcz kuriozalnej – liczby biegłych. Jest to zresztą niedobra praktyka, odradzana w literaturze (por. np. T. Grzegorczyk: *Kodeks Postępowania Karnego oraz ustawa o świadku koronnym*, pod red. T. Grzegorczyka, Wolters Kluwer, Warszawa, 2008, s. 466; P. Hofmański, S. Zabłocki: *Elementy metodyki pracy sędziego w sprawach karnych*, Wolters Kluwer, Warszawa, 201, s. 295). Sprzeczności mogą pojawić się również we wnioskach opinii różnych specjalistów (np. informatyka i elektronika) powołanych w tej samej sprawie, może również zdarzyć się, że w sprawie pojawi się opinia pozasądowa (zamówiona przez stronę) pozostająca w sprzeczności z konkluzjami opinii sądowej.

[232] Warto w tym kontekście zastanowić się nad pojawiającymi się od czasu do czasu postulatami utworzenia sądów specjalizowanych, których sędziowie mogliby uzyskać pewne wiadomości specjalne z zakresu dyscyplin, w których specjalizowałby się dany sąd. Wydaje się to o tyle sensowne, że istnieją wyspecjalizowane służby państwowe zajmujące się zwalczaniem szczególnych rodzajów przestępstw (np. Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Inspekcja Celna itd.), a nawet organy państwa powołane do orzekania w szczególnych rodzajach spraw (Izby Morskie). Można w tym kontekście przytoczyć znane a złośliwe powiedzenie o świadkach, którzy mówią o tym, na czym

biegłego polemizować[233], zmuszony jest natomiast, na którejś ze sprzecznych opinii oprzeć się wydając wyrok (sąd nie może pominąć wszystkich opinii biegłych i wbrew nim oprzeć ustaleń na własnym – odmiennym od wyrażonych w opinii lub opiniach – przekonaniu)[234].

Jedną z potencjalnych możliwości jest w takiej sytuacji zasięgnięcie metaopinii (zwanej również superekspertyzą). W literaturze i orzecznictwie przeważa sceptyczne nastawienie odnośnie do powołania „superbiegłego"[235] oraz do wspomnianych wcześniej sytuacji powoływania nadmiaro-

się nie znają, ale co widzieli, biegłych mówiących o tym, czego nie widzieli, ale na czym się znają i sędziach, którzy wypowiadają się o tym, na czym ani się nie znają, ani czego nie widzieli.

[233] Sąd mając wątpliwość co do opinii biegłego nie powinien z nią polemizować a zasięgnąć kolejnej opinii. Zob. wyrok Sądu Najwyższego z 3 maja 1982 r. (I KR 319/81).

[234] W wyroku z 14 marca 2007 r. (III UK 130/06) Sąd Najwyższy stwierdził: „Opinia biegłych dostarcza sądowi wiedzy specjalistycznej […] sąd nie może wbrew opinii biegłych oprzeć ustaleń w tym zakresie na własnym przekonaniu". W wyroku z 7 października 2009 r. (III KK 122/09) Sąd Najwyższy stwierdził: „jeżeli w sprawie zachodzi konieczność stwierdzenia okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy, które wymagają wiadomości specjalnych, sąd nie może zanegować wydanej opinii biegłego bez powołania innego biegłego. Sąd jest bowiem uprawniony wprawdzie do swobodnej oceny przeprowadzonych dowodów, ale nie do pominięcia przy tej ocenie uwzględnienia wskazań wiedzy specjalistycznej, zastępując je własną oceną zdarzeń, które wymagają opinii biegłego. Sąd, będąc uprawniony do swobodnej oceny dowodów, oceniając opinię biegłego może uznać, iż opinia biegłego jest niepełna lub niejasna albo, że zachodzi sprzeczność w samej opinii. Wtedy powinien wezwać ponownie tego biegłego lub powołać innych, aby uzupełnić opinię lub wyjaśnić sprzeczności".

[235] Zob. np.: J. Gurgul: *O swobodnej ocenie opinii biegłego*, „Prokuratura i Prawo" Nr 10/2013, s. 34–56, http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2013/10/3gurgul.pdf; P. Hofmański, S. Zabłocki: *Kodeks…*, op. cit., s. 294; T. Grzegorczyk: *Elementy…*, op. cit., s. 467; G. Kopczyński: *Konfrontacja…*, op. cit., s. 187 i nast. W tej ostatniej książce autor omawia szereg argumentów przeciwko możliwości stosowania „superekspertyzy":

- ✓ instytucja „superekspertyza" nie jest pojęciem ustawowym;
- ✓ uszczuplałaby ona swobodę oceny dowodów przez sąd;
- ✓ przedmiotem opinii w sprawie powinny być jej okoliczności, a nie trafność innej opinii.

wej liczby biegłych, w orzecznictwie można jednak znaleźć i przeciwne – tj. dopuszczające jakąś formę „superekspertyzy" – stanowiska[236]. Część autorów – za powołaną uchwałą Zgromadzenia Ogólnego Sądu Najwyższego – sugeruje, że rozwiązaniem może być w takich wypadkach konfrontacja biegłych[237]. Zasadniczo podzielając opinię o wyższości konfrontacji biegłych nad „superekspertyzą", należy podnieść zastrzeżenie, że konfrontacja jest szczególną formą przesłuchania, podczas gdy wyjaśnienie zaistniałych wątpliwości może wymagać od biegłego skorzystania z notatek,

Autor przytacza zdanie, że możliwość stosowania superekspertyzy dopuszcza się tylko w sytuacji, w której już przeprowadzona ekspertyza budzi zastrzeżenia, a powtórna ekspertyza nie jest możliwa np. z powodu zniszczenia wyniku badań.

O metaekspertyzie krytycznie wypowiedział się również Sąd Najwyższy w uchwale Zgromadzenia Ogólnego Sądu Najwyższego z 15 lipca 1974 r. (Kw. Pr. 2/74), punkt VII lit. g:

„W wypadku jednak, gdy opinia biegłego jest niejasna, zawiera w sobie sprzeczności albo też wykazuje, że nie uwzględniła całości materiału w badanej dziedzinie, należy domagać się przede wszystkim od dopuszczonego już biegłego opinii uzupełniającej lub innego stosownego wyjaśnienia swej opinii, a dopiero wtedy, gdyby to nie doprowadziło do pożądanego rezultatu, podejmować decyzję o powołaniu innego biegłego.

Również w wypadku, gdy opinie biegłych są rozbieżne, należy przede wszystkim domagać się, aby w drodze spowodowanej przez sąd konfrontacji biegli ustosunkowali się do opinii przeciwnych, wskazując na ich ewentualne błędy lub braki. Unikać natomiast należałoby odwoływania się do dalszych opinii innych jeszcze biegłych, a tym bardziej zwracania się o opinię specjalistyczną o opiniach dotychczas złożonych".

[236] Zob. postanowienie z 21 czerwca 2012 r. Sądu Apelacyjnego w Katowicach (II AKz 386/12): „Przepisy procedury karnej nie określają i nie mogą określać zakresu i metod badań specjalistycznych przeprowadzonych przez biegłych, w tej bowiem materii zasadnicze znaczenie mają specjalistyczne kwalifikacje biegłych. Sąd z natury nie może ingerować w te kwestie, albowiem nie posiada wiadomości specjalnych, warunkujących zajmowanie stanowiska w tej kwestii.

Jedynie w szczególnych sytuacjach, gdy zakres przeprowadzonych badań zdaje się wykraczać poza obszar zakreślony postanowieniem o dopuszczeniu dowodu z opinii biegłego, bądź też sąd poweźmie wątpliwość co do zasadności lub przydatności poszczególnych czynności biegłego składających się na przeprowadzoną ekspertyzę, może podjąć działania zmierzające do zweryfikowania i wyjaśnienia powyższych kwestii. Rzecz jednak w tym, że sąd nie może tego czynić w sposób samodzielny i arbitralny, albowiem z istoty rzeczy wkraczałby tym samym w zakres kompetencji biegłego. Środkiem do ustalenia przez sąd prawidłowości działań biegłego powołanego do wydania opinii w sprawie jest dopuszczenie innego biegłego, tylko w celu oceny prawidłowości wyboru metod oraz zasadności przeprowadzonych czynności, opisanych i wyjaśnionych w przedłożonej w sprawie opinii".

[237] I – przede wszystkim – wezwanie przez sąd biegłych do uzupełnienia czy wyjaśnienia już złożonych opinii.

literatury fachowej, czy nawet przeprowadzenia dodatkowych badań, co oczywiście nie jest możliwe w czasie przesłuchania[238]. Można spodziewać się, że konfrontacja nie przyniesie oczekiwanych skutków, gdy któryś z konfrontowanych biegłych podniesie argument konieczności sięgnięcia do literatury przedmiotu czy sprawdzenia czegoś w drodze eksperymentu. Co gorsza takie postawienie sprawy przez biegłego może zmniejszyć perswazyjność jego zdania, podczas gdy ta nie musi być przecież związana z prawdziwością stawianych tez. Można wreszcie spodziewać się, że sąd, który miał wątpliwości co do jasności (wydanej przecież na piśmie, a więc po uprzednim przygotowaniu i nadaniu odpowiedniej formy literackiej) opinii, nie uzna za bardziej klarowne efektów przesłuchania dwóch biegłych odnoszących się do wzajemnych wypowiedzi sformułowanych w mówionym języku fachowym. Niezależnie od rozważań nad dopuszczalnością czy pożytkiem z „superekspertyzy" w praktyce biegły może być zmuszony do odniesienia się do innych ekspertyz wydanych w tej samej sprawie, czy to w ramach postępowania (do opinii wcześniej powołanych biegłych[239], bądź do opinii prywatnych[240]), czy to poza nim (np. jeśli dokumentami znajdującymi się w aktach sprawy są ekspertyzy dotyczące tego

[238] Jakkolwiek art. 174 KPK zawierający zakaz substytuowania zeznań treścią pism, zapisków lub notatek urzędowych dotyczy zeznań świadka, a nie biegłego (inaczej: G. Kopczyński: *Konfrontacja*…, op. cit., s. 122).

[239] W szczególności w postępowaniu sądowym biegły może musieć odnieść się do opinii innego biegłego wydanej w postępowaniu przygotowawczym. Powołanie tego samego biegłego może być również niemożliwe z przyczyn obiektywnych (np. jego stanu zdrowia). Dyskusyjnym problemem (etycznym, bowiem z prawnego punktu widzenia nie ma tu przeciwwskazań) jest, czy ten sam biegły powinien opiniować w obu tych przypadkach: raz jako osoba powołana (i opłacana) przez prokuraturę, a drugi raz jako narzędzie sądu w procesie, gdzie ta sama prokuratura jest stroną. W literaturze podnoszony jest również problem możliwości pełnienia roli biegłych przez funkcjonariuszy wymiaru sprawiedliwości związanych organizacyjnie z prokuraturą. Z drugiej strony trudno spodziewać się, aby udało się zgromadzić odpowiednią liczbę specjalistów z zakresu poszczególnych technik kryminalistycznych, którzy nie są organizacyjnie związani z organami ścigania.

[240] Warto na marginesie zauważyć, że biegły pisząc opinię w sprawie, w której strona dostarczyła opinię pozasądową, nie jest zobligowany do odniesienia się do niej (chyba że taki zakres i przedmiot zostanie jawnie wskazany przez postanowienie sądu). Biegły nie musi bowiem (a często nawet nie powinien) w swoich opiniach polemizować ze stanowiskami stron procesowych, a opinia pozasądowa eksperta wynajętego przez stronę, przez tę stronę dostarczona ma taki charakter.

samego stanu rzeczowego, do którego powinien się odnieść biegły). Może to powodować pewien dyskomfort biegłego, szczególnie w przypadku niektórych zawodów o surowych kodeksach etycznych[241], czy też w niektórych środowiskach, nie zmienia to jednak faktu, że obowiązkiem biegłego jest mówić prawdę z całą sumiennością i bezstronnością. Nie oznacza to oczywiście konieczności obcesowej krytyki innych specjalistów, nawet jeśli popełnili oni błędy, z drugiej strony w przypadku błędów szczególnie rażących, popełnianych przez osoby wpisane na listy biegłych sądowych, zrozumiałe (co nie znaczy, że usprawiedliwione) są podejmowane przez niektórych biegłych próby informowania organu procesowego wręcz o podejrzeniu popełnienia przestępstwa przez powołanego poprzednio w sprawie biegłego, który np. zniszczył materiał dowodowy. Niestety kontrola działalności biegłych ma charakter bardzo wyrywkowy (nawet sam biegły z rzadka jedynie dowiaduje się, czy jego opinia została uwzględniona przez sąd, albo czy i w jakim zakresie sąd ma do niej zastrzeżenia[242]), tak więc nawet negatywna „superekspertyza" pozostaje zazwyczaj bez większych konsekwencji.

Sama sytuacja krytyki ekspertyzy (czy to w formie konfrontacji biegłych, czy polemiki ze strony „biegłego prywatnego") może spełniać pożyteczną rolę, podobnie jak pożyteczną rolę spełnia recenzja publikacji naukowej, oczywiście pod warunkiem, że krytyka taka prowadzona jest z pozycji me-

[241] Por. np. art. 52. ust. 2 Kodeksu etyki lekarskiej (dalej KodEL) „Lekarz powinien zachować szczególną ostrożność w formułowaniu opinii o działalności zawodowej innego lekarza, w szczególności nie powinien publicznie dyskredytować go w jakikolwiek sposób". Artykuł ten był zresztą wielokrotnie i słusznie krytykowany, a nawet został uznany przez Trybunał Konstytucyjny za niezgodny z Konstytucją, w zakresie, w jakim zakazuje zgodnych z prawdą i uzasadnionych ochroną interesu publicznego wypowiedzi publicznych na temat działalności zawodowej innego lekarza. Trybunał Konstytucyjny w wyroku z 23 kwietnia 2008 r. (SK 16/07) stwierdził: „Artykuł 52 ust. 2 KodEL w zw. z art. 15 pkt 1, art. 41 i art. 42 ust. 1 ustawy z 17 maja 1989 r. o izbach lekarskich w zakresie, w jakim zakazuje zgodnych z prawdą i uzasadnionych ochroną interesu publicznego wypowiedzi publicznych na temat działalności zawodowej innego lekarza, jest niezgodny z art. 54 ust. 1 w zw. z art. 31 ust. 3 i art. 17 ust. 1 Konstytucji oraz nie jest niezgodny z art. 63 Konstytucji".

[242] Do wyjątkowo rzadkich należy zaliczyć sytuacje, w których sądy dostarczają biegłym odpisy wyroków wraz z uzasadnieniami, w sprawach, w których biegli opiniowali, tak aby mogli dowiedzieć się, jaką rolę odegrała w sprawie ich opinia i jak została przez sąd oceniona. Zachowanie takie powinno być natomiast – zdaniem autora niniejszej monografii – powszechną praktyką.

rytorycznych i w sposób intelektualnie rzetelny. Warto również rozróżnić merytoryczną poprawność opinii od jej komunikatywności. Niejednokrotnie problemem opinii (i biegłego) jest nie jej nieprawidłowość, ale niejasność, która ma źródło w trudnościach komunikacyjnych między biegłym a sądem. Zdarza się, że rolą kolejnego biegłego („superbiegłego") w sprawie jest wyjaśnienie sądowi opinii napisanej przez poprzednika, bądź takie sformułowanie wniosków z jego badań, by stały się zrozumiałe dla organu procesowego i uczestników postępowania.

4 Opiniowanie w sprawach przestępstw komputerowych

Biegli informatycy opiniują w różnego rodzaju sprawach, w których konieczne jest ujawnienie różnego rodzaju informacji przetwarzanej w systemach informatycznych. Związane jest to z rolą, jaką urządzenia i systemy informatyczne odgrywają zarówno w zakresie działalności gospodarczej, jak i w stosunkach społecznych oraz przy okazji monitorowania ludzkiej aktywności, a także – z ogromnymi ilościami informacji przetwarzanej współcześnie[243]. Z punktu widzenia biegłego informatyka, szczególnie interesujące są przepisy odwołujące się *explicite* do pojęć informatycznych, w tym zagadnienia związane z opiniowaniem w sprawach karnych dotyczących tzw. przestępstw komputerowych. Dzieje się tak również dlatego, że przy okazji tych przestępstw zdefiniowano szereg pojęć użytecznych także w innych rodzajach spraw.

[243] Współcześnie przytłaczająca większość informacji ma postać elektroniczną: ponad 90% firmowych dokumentów jest tworzone, przeglądane i przechowywane w postaci elektronicznej, przy czym ponad 70% z tych informacji nigdy nie jest drukowane. Tzw. wszechświat cyfrowy (*digital universe*) w 2005 r. miał wielkość 130 EB (eksabajtów), w 2007 r. – 281 EB, w 2010 r. – 1,8 ZB (zetabajta), wykazuje więc wzrost wykładniczy. Urządzenia informatyczne odgrywają również coraz większą rolę w różnego rodzaju urządzeniach zabezpieczających i monitorujących, a te z kolei stają się nieodłączną częścią życia: w 2007 r. „cień cyfrowy", czyli ilość informacji cyfrowej generowanej na temat ludzi, przewyższyła ilość informacji generowanych przez nich samych. Zob. np.: P. Lyman, H.R. Varian, J. Dunn, A. Strygin, K. Swearingen: *How Much Information 2000?* University of Berkeley Raport, 2000, http://www2.sims.berkeley.edu/research/projects/how-much-info; K. Swearingen (ed.): *How Much Information 2003?* University of Berkeley Raport, (ed.) K. Swearingen, 2003, http://www2.sims.berkeley.edu/research/projects/how-much-info-2003; *IDC Whitepaper: The Diverse and Exploding Digital Universe. An Updated Forecast of Worldwide Information Growth Through 2011*, http://ww.ifap.ru/library/book268.pdf; *Digital Universe Program*, http://www.emc.com/leadership/programs/digital-universe.htm.

Niestety jakość polskiego prawa karnego w odniesieniu do tej akurat grupy przestępstw jest stosunkowo niska i sprawia wiele problemów zarówno samym biegłym, jak i organom wymiaru sprawiedliwości, stąd też przy przestępstwach komputerowych szczególnie długo trwa proces subsumpcji czynu (i już na tym etapie organ prowadzący postępowanie przygotowawcze korzysta często z pomocy biegłego). Dosyć często dochodzi również do sytuacji, w których w postępowaniu sądowym, sąd zmienia kwalifikację prawną czynu objętego aktem oskarżenia. Z tego też względu wydaje się wskazane, w miarę możliwości, szczegółowe omówienie przynajmniej najważniejszych przepisów i praktyki z tego zakresu.

Z czysto teoretycznego punktu widzenia z wykorzystaniem komputera można popełnić szereg przestępstw, komputer bowiem, będąc uniwersalnym narzędziem służącym do przechowywania, przetwarzania i przesyłania danych, może być użyty zarówno do działań z prawem zgodnych, jak i je naruszających; może też on sam, bądź owe dane, stać się obiektem ataku czy – szerzej mówiąc – działań przestępnych. Stąd też trudno jednoznacznie i precyzyjnie używać pojęć „przestępczość komputerowa”[244] czy „cyberprzestępczość”[245].

[244] Jako ciekawostkę można podać definicje terminu „przestępstwo komputerowe” zawarte w normach ISO:

„Przestępstwo komputerowe – przestępstwo popełnione za pomocą lub bezpośrednio dotyczące systemu przetwarzania danych lub sieci komputerowej” [PN-ISO/IEC 2382-8:2001-08.05.02].

„Przestępstwo komputerowe – naruszenie przepisów popełnione w wyniku wykorzystania, modyfikacji lub zniszczenia sprzętu komputerowego, oprogramowania lub danych” [PN-ISO/IEC 2382-1:1996- 01.07.02].

[245] Cybernetyka (ang. *cybernetics* z gr. *κυβερνητικός kybernētikós* „sternik”) jest nauką zajmującą się systemami sterowania oraz związanym z tym przetwarzaniem i przekazywaniem informacji. Stosunkowo często cybernetyka jest mylona z informatyką, w szczególności przez osoby zajmujące się innymi dziedzinami wiedzy. Prefix „cyber-” jest niezwykle popularny w mowie potocznej, z której przeniknął do języka potocznego i prawnego. Stało się tak np. z pojęciem cyberprzestrzeni (ang. *Cyberspace*). Samo słowo zostało użyte po raz pierwszy w opowiadaniu „Burning Chrome” autorstwa W. Gibsona, przy czym desygnat tego słowa był pierwotnie nieokreślony. Pojęcie „cyberprzestrzeni”, gdyby rozumieć je zgodnie z jego etymologią, jest z technicznego punktu widzenia co najmniej wątpliwe, po pierwsze z uwagi na różnice (przedmiotu materialnego, formalnego i metodologii) pomiędzy cybernetyką a informatyką, po wtóre – z uwagi na to, że trudno mówić o „przestrzeni cybernetycznej” (por. K. Liderman: *O zagrożeniach dla skutecznej ochrony informacji, przetwarzanej w sieciach*

Istnieje szereg ustaw, które penalizują w swoich zapisach działania mające związek z magazynowaniem, przetwarzaniem, udostępnianiem czy niszczeniem informacji (poczynając od przepisów dotyczących ochrony tajemnicy państwowej czy danych osobowych, poprzez zasady prowadzenia rachunkowości, aż do penalizacji rozpowszechniania, propagowania czy wyrażania poszczególnych treści np. publicznego nawoływania do waśni religijnych czy narodowościowych) oczywiście zaś niemalże wszędzie tam, gdzie mowa jest o informacji, można do jej przetwarzania użyć komputerów bądź innych urządzeń informatycznych. Nawet gdyby zawęzić rozważania do przepisów, w których *explicite* występują pojęcia komputera czy systemu teleinformatycznego, katalog obowiązujących przepisów byłby bardzo bogaty. Andrzej Adamski[246] rozważa zagadnienia zebrane w art. 267, 268, 269, 270, 276, 303, 310, 278, 293, 287, 285, 130 i 165 KK oraz art. 49, 50, 51, 52, 53 i 54 ustawy o ochronie danych osobowych (dalej UODO). Należałoby listę tę uzupełnić choćby o artykuły KK wprowadzone doń w ramach nowelizacji (268a, 269a i 269b), jak również o artykuły ustawy z 4 lutego1994 r. o prawie autorskim i prawach pokrewnych (dalej PrAut) znajdujące zastosowanie w ochronie prawnoautorskiej oprogramowania komputerowego[247], o przepisy UONUDE czy ustawy Prawo Telekomunikacyjne (dalej PrTel). W literaturze przedmiotu proponowane są różne kwalifikacje typologiczne tego rodzaju przestępstw. I tak Konwencja Rady Europy o cyberprzestępczości

i systemach teleinformatycznych, powodowanych nowomową, Konferencja Cyberspace 2009, WAT 2009), niemniej stosowane jest zarówno w języku potocznym, jak w aktach prawnych (zob. ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw; dalej UUSW), a także normach międzynarodowych (zob. [ISO/IEC 270032]). Podobnie używa się określeń „cyberprzestępczość" czy „cyberterroryzm" (zob. np.: A. Suchorzewska: *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, 2010; J. Dworzecki: *Terroryzm jako zagrożenie współczesnego świata*, Zeszyt Naukowy „Apeiron" Nr 5, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego w Krakowie, Kraków 2011, s. 181–232).

[246] A. Adamski: *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000.

[247] Por. np. A. Siluszek: *Przestępstwa komputerowe*, „PC Kurier" 2000/8/42, http://www.pckurier.pl/archiwum/artykuly/siluszek_andrzej/2000_08_42, s. 33; S. Bukowski: *Projekt zmian Kodeksu karnego. Dostosowanie do Konwencji o cyberprzestępczości* „Gazeta Sądowa" kwiecień 2004, http://www.prawo.lex.pl/czasopisma/gs/pzmiankk.html.

(dalej KREoC) w poszczególnych tytułach i zawartych w nich artykułach wyróżnia:

- ✓ Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (Tytuł 1):
  - o nielegalny dostęp (art. 2);
  - o nielegalne przechwytywanie danych (art. 3);
  - o naruszenie integralności danych (art. 4);
  - o naruszenie integralności systemu (art. 5);
  - o niewłaściwe użycie urządzeń (art. 6);
- ✓ (Tytuł 2) Przestępstwa komputerowe:
  - o fałszerstwo komputerowe (art. 7);
  - o oszustwo komputerowe (art. 8);
- ✓ (Tytuł 3) Przestępstwa ze względu na charakter zawartych informacji:
  - o przestępstwa związane z pornografią dziecięcą (art. 9);
- ✓ (Tytuł 4) Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych:
  - o przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (art. 10).

W literaturze przedmiotu przestępstwa związane z posiadaniem, przechowywaniem czy przesyłaniem tzw. nielegalnych treści (ze względu na charakter zawartych informacji)[248] nazywa się czasami „kontentowymi" (ang. *content* – treść, zawartość), natomiast przestępstwa odpowiadające wspominanemu powyżej Tytułowi 1 Konwencji o cyberprzestępczości – przestępstwami CIA (ang. *confidentionality*, *integrity*, *availability* – poufność, integralność, dostępność).

Polska podpisała Konwencję o cyberprzestępczości 23 listopada 2001 r., natomiast nie ratyfikowała jej do chwili powstania niniejszej monografii

[248] W szczególności dotyczy to – wymienionej *explicite* w Tytule 3 Konwencji – pornografii dziecięcej, niemniej może dotyczyć wszelkich sytuacji, w których komputer został użyty do przetwarzania jakiegoś rodzaju „informacji zakazanej", to jest – ściśle rzecz ujmując – do nielegalnego przesyłania, rozpowszechniania, przetwarzania czy wytwarzania informacji (np. w Protokole Dodatkowym do Konwencji wymienione są czyny o charakterze rasistowskim i ksenofobicznym popełniane przy użyciu systemów komputerowych, niemniej może to być również np. nielegalnie przesyłana informacja niejawna itp.).

(2014 r.). Poniżej (Tabela 1) zestawiono artykuły Konwencji o cyberprzestępczości i odpowiadające im (w pewnym przybliżeniu) przepisy KK.

Tabela 1. Orientacyjne odwzorowanie przepisów Konwencji o cyberprzestępczości na przepisy Kodeksu Karnego

Konwencja o cyberprzestępczości	**Przepisy KK**
Nielegalny dostęp – Art. 2 Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego dostępu do całości lub części systemu informatycznego. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym.	**Art. 267 § 2** Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
Nielegalne przechwytywanie danych – Art. 3 Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego przechwytywania za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne. Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione z nieuczciwym zamiarem lub w związku z systemem informatycznym, który jest połączony z innym systemem informatycznym.	**Art. 267 § 1** Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. **Art. 267 § 3** Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
Naruszenie integralności danych – Art. 4 1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych. 2. Strona może zastrzec sobie prawo wprowadzenia wymogu, że zachowanie opisane w ustępie l musi skutkować poważną szkodą.	**Art. 268** **§ 1.** Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. **§ 2.** Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. **§ 3.** Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. **Art. 268a** **§ 1.** Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca

	lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3. **§ 2.** Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Naruszenie integralności systemu – Art. 5 Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnego, bezprawnego poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych.	**Art. 269a** Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Niewłaściwe użycie urządzeń – Art.6 1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwo w jej prawie wewnętrznym, umyślnych i bezprawnych: a. produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania: i. urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5; ii. hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2 -5; oraz b. posiadania jednostki wymienionej powyżej w punktach a. i. lub ii. z zamiarem wykorzystania w celu popełnienia któregokolwiek z przestępstw określonych zgodnie z artykułami 2-5. Strona może w swoim prawie wprowadzić wymóg, że odpowiedzialność karna dotyczy posiadania większej ilości takich jednostek. 2. Niniejszego artykułu nie należy interpretować jako mającego na celu pociągnięcia do odpowiedzialności karnej w przypadku, kiedy produkcja, sprzedaż, pozyskiwanie z zamiarem wykorzystania, importowanie, dystrybucja lub inne udostępnianie lub posiadanie, o którym mowa w ustępie l niniejszego artykułu, nie jest dokonywane w celu popełnienia przestępstwa określonego zgodnie z artykułami 2-5 niniejszej Konwencji, jak w przypadku dozwolonego testowania lub ochrony systemu informatycznego. 3. Każda Strona może zastrzec sobie prawo do niestosowania ustępu l niniejszego artykułu, pod warunkiem, że zastrzeżenie to nie dotyczy sprzedaży, dystrybucji	**Art. 269b** **§ 1.** Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3. **Art. 269b** **§ 2.** W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

lub innego udostępniania jednostek wymienionych w ustępie 1.a.ii.	
Fałszerstwo komputerowe – Art. 7 Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego wprowadzania, dokonywania zmian, wykasowywania lub usuwania danych informatycznych, w wyniku czego powstają dane nieautentyczne, które w zamiarze sprawcy mają być uznane lub wykorzystane w celach zgodnych z prawem jako autentyczne, bez względu na to czy są one możliwe do bezpośredniego odczytania i zrozumiałe. Strona może wprowadzić wymóg, że odpowiedzialność karna dotyczy działania w zamiarze oszustwa lub w podobnym nieuczciwym zamiarze.	**Art. 269** **§ 1.** Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. **Art. 269** **§ 2.** Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych.
Oszustwo komputerowe – Art. 8 Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnego, bezprawnego spowodowania utraty majątku przez inną osobę poprzez: a. wprowadzenie, dokonanie zmian, wykasowanie lub usunięcie danych informatycznych, b. każdą ingerencję w funkcjonowanie systemu komputerowego, z zamiarem oszustwa lub nieuczciwym zamiarem uzyskania korzyści ekonomicznych dla siebie lub innej osoby.	**Art. 287** **§ 1.** Kto, w celu osiągniecia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
Przestępstwa związane z pornografią dziecięcą – Art. 9 1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, umyślnych, bezprawnych: a. produkowania pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego; b. oferowania lub udostępniania pornografii dziecięcej za pomocą systemu informatycznego; c. rozpowszechniania lub transmitowanie pornografii dziecięcej za pomocą systemu informatycznego; d. pozyskiwanie pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby; e. posiadanie pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych. 2. Dla celów powyższego ustępu l pojęcie „pornografia dziecięca" obejmuje materiał pornograficzny, który w sposób widoczny przedstawia: a. osobę małoletnią w trakcie czynności wyraźnie seksualnej; b. osobę, która wydaje się być nieletnią, w trakcie czynności wyraźnie seksualnej;	**Art. 202** **§ 3.** Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od lat 2 do 12. **Art. 202** **§ 4.** Kto utrwala treści pornograficzne z udziałem małoletniego poniżej lat 15, podlega karze pozbawienia wolności od roku do lat 10. **Art. 202** **§ 4a.** Kto przechowuje, posiada lub uzyskuje dostęp do treści pornograficznych z udziałem małoletniego, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. **Art. 202** **§ 4b.** Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

c. realistyczny obraz przedstawiający osobę małoletnią w trakcie czynności wyraźnie seksualnej. 3. Dla celów powyższego ustępu 2, pojęcie „osoba małoletnia" obejmuje wszystkie osoby poniżej 18 roku życia. Strona może wprowadzić wymóg niższej granicy wieku, która nie może być niższa niż 16 lat. 4. Każda ze Stron może zastrzec sobie prawo niestosowania, w całości lub w części, ustępu l.d. i e. oraz ustępu 2.b. i c.	**Art. 202** **§ 4c.** Karze określonej w § 4b podlega, kto w celu zaspokojenia seksualnego uczestniczy w prezentacji treści pornograficznych z udziałem małoletniego.
Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych – Art. 10 1. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń prawa autorskiego zdefiniowanego w prawie danej Strony zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Aktu Paryskiego z dnia 24 lipca 1971 roku zmieniającego Konwencję Berneńską o ochronie dzieł literackich i artystycznych, Porozumienia w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o prawach autorskich, z wyłączeniem praw osobistych przewidzianych przez te Konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego. 2. Każda Strona podejmie takie środki prawne i inne, jakie okażą się niezbędne dla uznania za przestępstwa w jej prawie wewnętrznym, naruszeń praw pokrewnych zdefiniowanych w prawie danej Strony, zgodnie z podjętymi przez nią zobowiązaniami wynikającymi z Międzynarodowej Konwencji o ochronie wykonawców, producentów fonogramów organizacji nadawczych zawartej w Rzymie (Konwencja Rzymska), Umowy w sprawie handlowych aspektów praw własności intelektualnej oraz Traktatu Światowej Organizacji Własności Intelektualnej o wykonaniach i fonogramach, z wyłączeniem praw osobistych przewidzianych przez te Konwencje, jeżeli popełnione są umyślnie, na skalę komercyjną i za pomocą systemu informatycznego. 3. Strona może zastrzec sobie prawo do niepociągania do odpowiedzialności karnej na podstawie ustępów l i 2 niniejszego artykułu w pewnych przypadkach, pod warunkiem, że istnieją inne skuteczne środki prawne oraz że zastrzeżenie to nie stanowi odstępstwa od międzynarodowych zobowiązań Strony określonych w międzynarodowych instrumentach, wymienionych w ustępach l i 2 niniejszego artykułu.	**Przepisy dotyczące ochrony praw autorskich zostały zawarte w Prawie Autorskim.**

Klasyfikacja zastosowana w Konwencji o cyberprzestępczości została wykorzystana w dalszej części niniejszej monografii (rozdziały 4.3–4.10), przy czym zagadnienia przestępstw kontentowych na przykładzie art. 202 KK omówiono w kolejnym rozdziale (5.1). Należy jednak wspomnieć, że istnieją również inne klasyfikacje „przestępstw komputerowych"[249]. Stosunkowo często wyróżnia się przestępstwa komputerowe oraz przestępstwa dokonywane przy użyciu komputera[250]. Zasadniczą różnicą jest w tym wypadku użycie komputera (systemu teleinformatycznego, programów komputerowych) bądź to jako celu, bądź to jako narzędzia działania[251].

Bogdan Fischer proponuje schemat rozkładu i nakładania się przestępstw komputerowych zilustrowany jak na rysunku na następnej stronie.

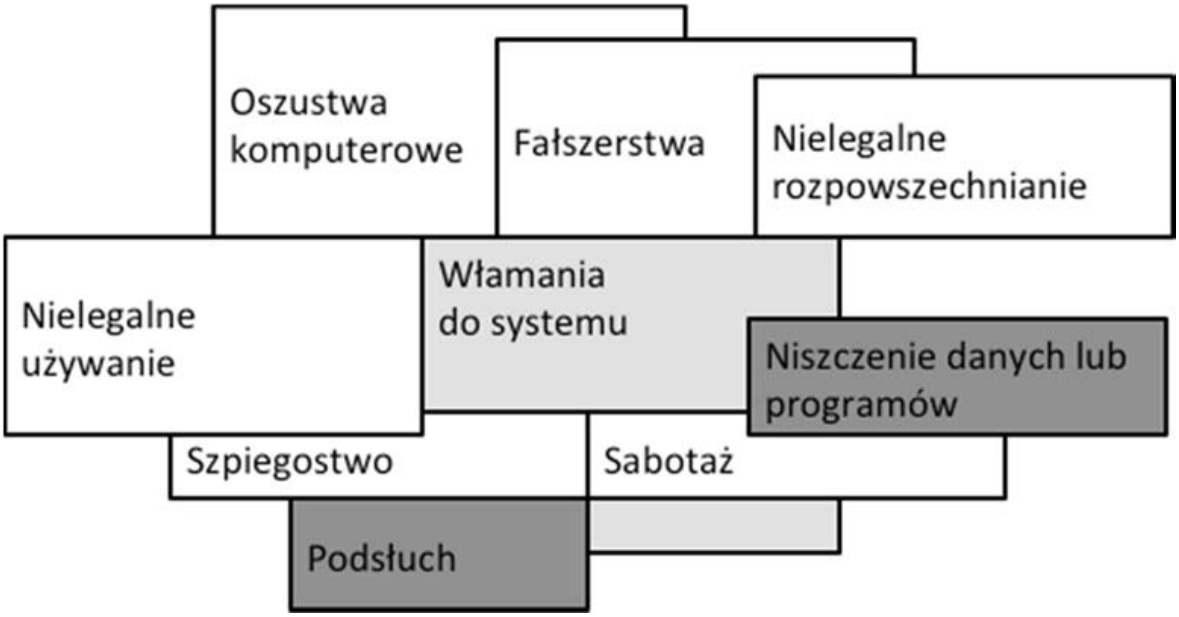
[249] W pracy M. Sowy omówiono szereg klasyfikacji proponowanych w literaturze przedmiotu i zaproponowano wyróżnienie trzech grup przestępstw komputerowych:

- ✓ przestępstwa niemożliwe do popełnienia poza środowiskiem komputerowym (przestępstwa komputerowe *sensu stricto*);
- ✓ przestępstwa tradycyjnie penalizowane przepisami prawa karnego, w przypadku których komputer ułatwia ich popełnianie w nowy lub dotychczasowy sposób (przestępstwa komputerowe *sensu largo*);
- ✓ przestępstwa, w przypadku których komputer jest wykorzystywany przez sprawców, lecz jego rola jest ściśle poboczna.

(M. Sowa: *Przestępczość komputerowa – badanie celowości i skuteczności kryminalizacji*, Kraków 2005, praca doktorska, maszynopis, http://m-sowa.pl/MSowa-przestepczosc-komputerowa.pdf; s. 59).
Jeszcze inne klasyfikacje przestępstw komputerowych można znaleźć np. w pracy A. Płaza: *Przestępstwa komputerowe*, Rzeszów 2000, praca magisterska, maszynopis, http://vagla.pl/skrypts/mgr_a_plaza.pdf (s. 7 i nast.).

[250] Por. np. J. Warylewski*: Przestępstwo oszustwa komputerowego (art. 287 KK) — podstawowe zagadnienia teoretycznoprawne i praktyczne*, http://panda.bg.univ.gda.pl/%7Ewaryl/ok.htm; S. Bukowski: *Projekt*…, op. cit.; M. Szmit, I. Politowska: *O artykule 267 Kodeksu Karnego oczami biegłego*, „Prawo Mediów Elektronicznych" (8), dodatek do „Monitora Prawniczego" Nr 16/2008, s. 34–40; K.J. Jakubski: *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" Nr 12/1996.

[251] Zob. np.: B. Fischer: *Przestępstwa komputerowe i ochrona informacji*, Zakamycze, Kraków 2000, s. 24; M. Szmit: *Bezpieczeństwo Informatyczne* [w:] I. Staniec, J. Zawiła-Niedźwiecki: *Zarządzanie ryzykiem operacyjnym*, C.H. Beck, Warszawa 2008, s. 201–228; M. Sowa: *Przestępczość*…, op. cit.



Rysunek 1. Rozkład i nakładanie się przestępstw komputerowych[252].

4.1 Terminologia

Mówiąc o terminologii w odniesieniu do przestępstw komputerowych należy rozróżnić terminologię stosowaną w informatyce (a więc przede wszystkim terminologię znormalizowaną zawartą w Polskich Normach i w normach międzynarodowych ISO, w tym w normach dotyczących bezpieczeństwa informacji) oraz terminologię stosowaną w aktach prawa krajowego i międzynarodowego.

Pierwszymi i poniekąd podstawowymi pojęciami, które mogą sprawiać trudności przy rozumieniu przepisów prawa są pojęcia informacji oraz danych.

Słowo „informacja" wywodzi się z łacińskiego zrostu *informare* („in" + „formare") – kształtować, odciskać formę bądź przedstawiać, wyobrażać, określać. „Informatio" oznaczało (w różnych epokach) wyobrażenie, a także

[252] Źródło: B. Fischer: *Przestępstwa…*, op. cit., s. 33.

znaczenie pojedynczego wyrazu, proces formowania i jego rezultat, jak również pouczenie oraz rezultat pouczenia[253]. W różnych definicjach informacji powtarzają się odwołania do procesu przekazywania treści (łac. *forma*), np.:

- ✓ „pewna treść będąca opisem, poleceniem, nakazem lub zakazem, przekazywana w jakikolwiek sposób od nadawcy o odbiorcy"[254];
- ✓ „relacja niematerialna, zachodząca jednocześnie między trzema elementami: A. odtwarzanym obiektem rzeczywistości społecznej, B. tezaurusem punktu A, C. społecznym nastawieniem do A i B"[255];
- ✓ „relacja definiowana na elementach komunikatu K (…). Jest to treść, czyli desygnat oznaczony jako informacja. Informacja na tym poziomie nazywa się informacją datalogiczną i jest zapisywana jako I(K), dla podkreślenia informacji, jaką dostarcza komunikat K niezależnie od odbiorcy U. Aspekt pragmatyczny informacji wymaga uwzględnienia procesu jej odbioru przez użytkownika. W tym celu stosuje się zapis (…): I (K, U, Q)"[256] (K oznacza komunikat, U-odbiorcę informacji, zaś Q-kontekst).

Ta ostatnia definicja jest to tzw. definicja infologiczna informacji. Samo pojęcie infologii oraz rozróżnienie pomiędzy datalogicznym a infologicznym poziomem ujęcia informacji zostało spopularyzowane przez B. Sungardena w pracy doktorskiej[257], jakkolwiek współcześnie nie ma powszechnie przyjętej definicji infologii. Jak się wydaje „podejście infologiczne" koncentruje się na podkreślaniu znaczenia informacji oraz procesów jej komunikowania i percepcji przez użytkownika, wpływu informacji na podejmowane decyzje i ludzkie działania itd.[258] Podejście to

[253] Zob. np.: Ł. Kister: *Bezpieczeństwo informacyjne infrastruktury krytycznej*, „Terroryzm" Nr 1/2010, Collegium Civitas, Warszawa 2010, s. 69.

[254] J. Gościński: *Zarys sterowania ekonomicznego*, PWN, Warszawa 1977.

[255] Zob. np.: http://www.encyklopedia.biolog.pl/index.php?haslo=Informacja. Jest to tzw. „cybernetyczna definicja informacji".

[256] Zob. np.: B. Stefanowicz: *Informacja*, Oficyna Wydawnicza SGH, Warszawa 2004.

[257] B. Sungarden: *An Infological Approach to Data Bases*, Ph.D. Thesis, https://sites.google.com/site/bosundgren/my-life/AnInfologicalApproachtoDataBases.pdf?attredirects=0.

[258] Zob. np.: L.F. Korzeniowski: *Firma w warunkach ryzyka gospodarczego*, EAS, Kraków 2002, s. 176 i nast.

wyróżnia dwa poziomy rozumienia pojęcia informacji: datalogiczny (informacja to treść komunikatu, niezależnie od znaczenia, jaki nadaje jej odbiorca komunikatu) oraz infologiczny (informacja to subiektywne znaczenie, jakie treści komunikatu nadaje jego odbiorca)[259].

Samo „podejście infologiczne" jest istotne w kontekście jego wpływu (w szczególności dość drobiazgowego i nie zawsze intuicyjnie zrozumiałego rozróżniania pomiędzy „danymi" a „informacją", skądinąd pojęciami znanym już z teorii informacji[260]) na redakcję przepisów prawa, np. Kodeksu karnego.

Z technicznego punktu widzenia (dla języka informatyki) najważniejsze są definicje podane w Polskich Normach, w szczególności w normach nomenklaturowych z serii PN-ISO/IEC 2382-X.

Polska Norma [PN-ISO/IEC 2382-1:1996] zawiera odpowiednio definicje:

„Dane – reprezentacja informacji mająca interpretację, właściwa do komunikowania się, interpretacji lub przetwarzania.

Uwagi

1. dane mogą być przetwarzane przez człowieka lub za pomocą środków automatycznych

2. patrz rysunek 1"[261]

oraz

„Informacja (w przetwarzaniu informacji) – Wiedza dotycząca obiektów, takich jak fakty, zdarzenia, przedmioty, procesy lub idee, zawierająca koncepcje, która w określonym kontekście ma określone znaczenie

Uwaga – patrz rysunek 1"[262],

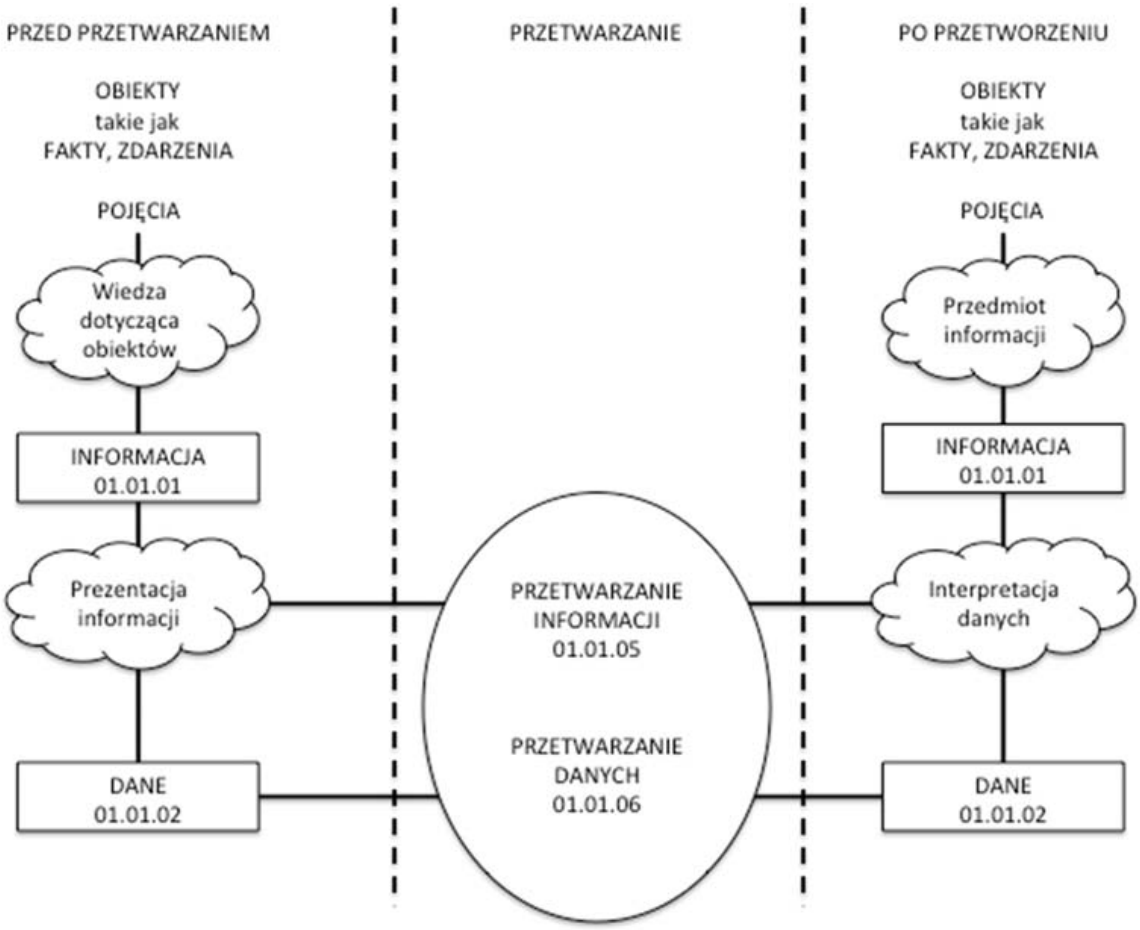
definicje te uzupełnione są rysunkiem jak na następnej stronie (rysunek 2).

[259] Zob. A. Lotko: *Źródła różnorodności informacji w marketingu relacyjnym*, „Studia i Materiały Wydziału Zarządzania UW" Nr 1/2007, s. 67–74, http://www.sim.wz.uw.edu.pl/pl/numer/numer-1-2007.

[260] Pojęcie „teorii informacji" związane jest z pracami C.E. Shannona z końca lat 40. XX w.

[261] PN-ISO/IEC 2382-1:1996-01.01.02.

[262] PN-ISO/IEC 2382-1:1996-01.01.01.



Rysunek 2. Wzajemne relacje między informacją a danymi[263].

Z punktu widzenia normy, przetwarzanie informacji jest więc pojęciem szerszym niż przetwarzanie danych (to ostatnie jest wykonywaniem operacji na danych, natomiast przetwarzanie informacji może zawierać oprócz przetwarzania danych inne operacje, jak np. automatyzację prac biurowych), dane natomiast są reprezentacją informacji, zarówno jednak informacja, jak i dane mogą być przetwarzane, jak również dane posiadają interpretację.

Różnica między rozumieniem informacji i danych na sposób informatyczny i prawniczy może prowadzić do brzemiennych w skutki nieporozumień, niektóre bowiem dyspozycje KK odwołują się do „danych", a inne do „informacji", co może implikować i takie rozumienie, że jedne z przestępstw

[263] Źródło: [PN-ISO/IEC 2382-1:1996] rysunek 1.

można popełnić w odniesieniu do informacji (rozumianej jako treść komunikatu), a inne – do danych (rozumianych jako zapisy)[264].

Pojęcia poufność, integralność, dostępność związane są z pojęciem bezpieczeństwa informacji, definiowanym w normie PN-ISO/IEC 17799:2007 jako zachowanie poufności, integralności i dostępności informacji, a dodatkowo także innych własności jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność[265]. Z kolei te własności bezpieczeństwa informacji definiowane są w normach odpowiednio jako:

- ✓ **poufność** (ang. *confidentiality*), własność polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, przedmiotom lub procesom[266];
- ✓ **integralność** (ang. *integrity*), własność polegająca na zapewnieniu dokładności i kompletności aktywów[267];
- ✓ **dostępność** (ang. *availability*), własność bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu[268].

Dodatkowe atrybuty bezpieczeństwa informacji definiowane są w normach jako:

- ✓ **autentyczność** (ang. *authenticity*), właściwość zapewniająca, że tożsamość podmiotu lub zasobu jest taka jak deklarowana[269];
- ✓ **rozliczalność** (ang. *accountability*) – właściwość, która zapewnia, że określone działania dowolnego podmiotu mogą być jednoznacznie przypisane temu podmiotowi[270];

[264] Zob. przypis 277.
[265] PN-ISO/IEC 17799:2007 – 2.5.
[266] PN-ISO/IEC 27001:2007 – 3.3.
[267] PN-ISO/IEC 27001:2007 – 3.8. Rozróżnia się dodatkowo integralność danych oraz integralność systemu.
[268] PN-ISO/IEC 2382-8:2001 – 08.01.17.
[269] PN-I-02000:2002-3.1.008. Procesem prowadzącym do stwierdzenia autentyczności jest uwierzytelnienie (ang. *authentication*), czyli działanie weryfikowania deklarowanej tożsamości jednostki [PN-I-02000:2002 – 3.4.105].
[270] PN-I-02000:2002-3.1.095.

- ✓ **niezaprzeczalność** – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie[271];
- ✓ **niezawodność** (ang. *reliability*) – zdolność jednostki funkcjonalnej do wykonywania wymaganej funkcji w danych warunkach i w danym przedziale czasu[272].

Oczywiście katalog własności bezpieczeństwa informacji nie jest katalogiem zamkniętym (jako przykład można wymienić – pożądaną, np. podczas badań statystycznych anonimowość[273], którą można również traktować jako własność bezpieczeństwa informacji, niejako przeciwstawną rozliczalności).

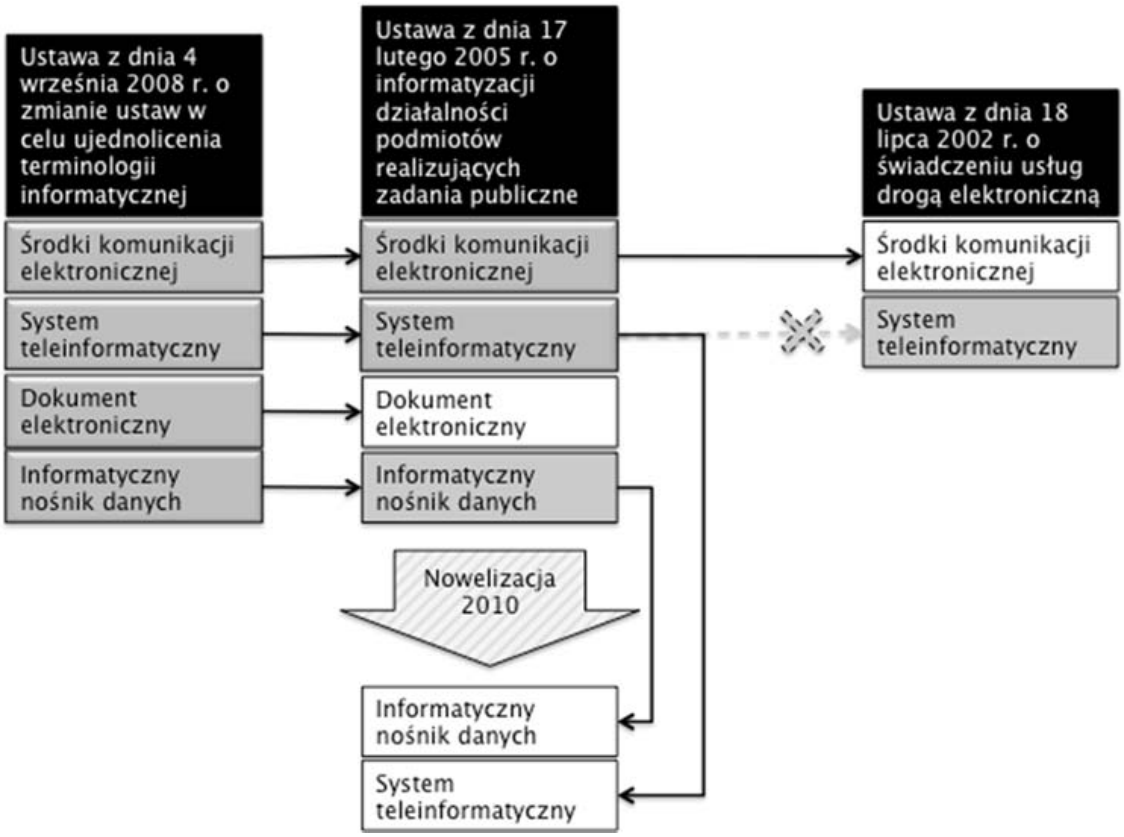
W języku prawnym terminologia informatyczna została częściowo usystematyzowana ustawą z 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (dalej UzmwCUJ). W swoim pierwszym artykule ustawa ta wprowadza w szeregu ustaw cztery pojęcia: „informatyczny nośnik danych", „dokument elektroniczny", „system teleinformatyczny" oraz „środki komunikacji elektronicznej" użyte w art. 3 pkt 1-4 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (dalej UOINF). Ta ostatnia zawierała podówczas (w chwili wejścia w życie UzmwCUJ) definicje informatycznego nośnika danych i dokumentu elektronicznego, zaś co do systemu teleinformatycznego i środków komunikacji elektronicznej odsyłała do ustawy o świadczeniu usług drogą elektroniczną (dalej UŚUDE).

W roku 2010 znowelizowano UOINF. Po nowelizacji zawiera ona inną niż pierwotna (ta z 2005 r.) definicję informatycznego nośnika danych (skreślono słowa „lub analogowej" – mowa o postaci danych przechowywanych na tym nośniku) i własną definicję systemu teleinformatycznego (niemal zresztą identyczną z definicją z ustawy o świadczeniu usług drogą elektroniczną (zob. rysunek 3 na kolejnej stronie). Dodatkowo definicja ta zawiera w sobie odwołanie do definicji urządzenia końcowego wziętej z ustawy PrTel.

[271] PN-I-02000:2002-3.1.054. Norma ISO/IEC 27000:2014-2.54 podaje szerszą definicję, dotyczącą uczestnictwa w zdarzeniu lub podjęcia działania: „ability to prove the occurrence of a claimed event or action and its originating entities".

[272] PN-ISO/IEC 2382-14:2001-14.01.03.

[273] Zasada, z której wynika, że podmiot może wykorzystywać zasób lub usługę bez ujawniania swojej tożsamości [PN-I-02000:2002-3.1.002].



Rysunek 3. Zmiany w definicjach po nowelizacji ustawy o informatyzacji[274].

Konsekwencje zmian w definicjach mogą być daleko idące, bowiem np. to czy jakiś czyn spełnia ustawowe znamię zawarte w dyspozycji art. 268 § 2 KK, zależy od tego, jaka definicja informatycznego nośnika danych obowiązuje w ustawie o informatyzacji[275]. Każda zmiana w tejże ustawie (bądź w ustawie, do której ona w zakresie przyjętych definicji odsyła) będzie skutkowała zmianą rozumienia przepisów Kodeksu karnego (i pozostałych, wyżej wymienionych ustaw). Stąd też np. w przypadku tworzenia aktu oskarżenia trzeba wiedzieć nie tylko o tym, jaka definicja obowiązuje obecnie, ale i jaka obowiązywała w chwili popełnienia inkryminowanego czynu i – zgodnie z art. 4 KK – stosować ustawę względniejszą dla sprawcy.

[274] Źródło: opracowanie własne.

[275] Przed nowelizacją definicja ta obejmowała urządzenia i materiały służące do przechowywania danych analogowych i cyfrowych, po nowelizacji – wyłącznie cyfrowych.

W momencie pisania niniejszej monografii odpowiednie definicje brzmiały:

- ✓ informatyczny nośnik danych – materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej (art. 2 ust. 1 UOINF);
- ✓ dokument elektroniczny – stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych (art. 2 ust. 2 UOINF);
- ✓ system teleinformatyczny – zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy PrTel;
- ✓ środki komunikacji elektronicznej – rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną.

4.2 Statystyki przestępczości komputerowej

Istniejące statystyki wymiaru sprawiedliwości nie odzwierciedlają w pełni obrazu przestępczości, niemniej nawet z tak niekompletnych danych można dostrzec, że liczba zarówno stwierdzonych przestępstw, jak i skazań jest stosunkowo niewielka nie tylko w liczbach bezwzględnych, ale i procentowo wśród wszystkich przestępstw. Na przykład Ministerstwo Sprawiedliwości[276] publikuje tylko dane o prawomocnie skazanych dorosłych według rodzajów przestępstw (czynu głównego) i wymiaru kary (Tabela 2), co oczywiście nie pozwala na wnioskowanie niczego np. o liczbie warunkowych umorzeń, skazanych małoletnich czy całkowitej liczby czynów wypełniających ustawowe znamiona czynu zabronionego (w szczególności nie da się

[276] Zob. http://bip.ms.gov.pl/pl/dzialalnosc/statystyki.

wyznaczyć liczby przestępstw, które nie są dla skazanych czynami głównymi). Statystyki policyjne prowadzone są w układzie chronologicznym według daty stwierdzenia przestępstwa, natomiast statystyki Ministerstwa Sprawiedliwości – według daty skazania.

Tabela 2. Liczba stwierdzonych przestępstw (prawa kolumna) i wszczętych postępowań (lewa kolumna) według statystyk policyjnych[277].

Rok	Art. 267 § 1-3[278] KK		Art. 268 i 268a KK		Art. 269 § 1-2 KK		Art. 269a KK		Art. 269b KK		Art. 287 § 1–2 KK	
	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw
2013	2203	1655	765	589	14	9	37	34	42	28		
2012	1657	1513	796	884	9	5	35	30	21	27	1285	
2011	1583	948	885	629	3	5	38	30	38	29	1012	
2010	1194	1102	690	479	7	0	22	18	35	71	838	
2009	982	645	555	1115	6	2	34	243	23	18	673	
2008	694	505	366	249	6	2	13	13	12	12	472	404
2007	616	384	244	168	6	0	11	11	4	4	322	492
2006	538	370	201	136	3	4	19	19	9	9	285	444
2005	430	260	152	98	2	3	1	1	6	6	326	568
2004	378	248	105	89	12	0					229	390
2003	362	232	114	138	2	2					219	168
2002	294	215	89	167	6	12					114	368
2001	259	175	60	118	9	5					59	279
2000	249	240	66	48	7	5					127	323
1999	182	113	59	49	10	1					52	217

Dodatkowo statystyki policyjne prowadzone są na poziomie artykułów Kodeksu karnego (bądź nawet wyższym: np. łącznie artykułów 268 i 268a KK), tak więc np. nie da się rozróżnić osób uzyskujących dostęp do systemu informatycznego od osób otwierających zamknięte pismo (art. 267 § 1 KK).

[277] Źródło: http://www.statystyka.policja.pl/st/kodeks-karny; A. Suchorzewska: *Ochrona…*, op. cit., s. 100. W 2010 r. policja zmieniła sposób prezentacji statystyk, w miejsce dotychczasowych (liczby stwierdzonych przestępstw) prezentując liczbę wszczętych postępowań, w 2014 r. policja wprowadziła publikację obu tych wielkości na swoich stronach.

[278] W obecnej (2014 r.) wersji stron policyjnych podana jest informacja „par. 1–4".

Tabela 3. Prawomocnie skazani dorośli ogółem wg rodzajów przestępstw – czyn główny[279].

Rok	Art. 267 KK						Art. 268 KK				Art. 268a KK		Art. 269 KK		Art. 269a KK	Art. 269b KK			Art. 287 KK		
	Art. 267 §1 KK	Art. 267 §2 KK	Art. 267 §3 KK	Art.267 §3 w zw. z §1 KK	Art.267 §3 w zw. z §1 (pokrzyw. mał.) KK	Art. 267 § 4 KK	Art. 268 §1 KK	Art. 268 §2 KK	Art. 268 §3 KK	Art. 268 §3 w zw. z §1 KK	Art. 268a §1 KK	Art. 268a §2 KK	Art. 269 §1 KK	Art. 269 §2 KK	Art. 269a KK	Art. 269b §1 KK	Art.269b §1 w zw. z art. 268a §1 KK	Art.269b §1 w zw. z art.269a KK	Art. 287 §1 KK	Art. 287 §2 KK	Art. 287 §3 KK
2010	52		11	#	#	#	12	11	#	#	33	#	#	#	#	#			43	#	#
2009	42	#	#	#		#	13	5			25			#	#	#			45	4	#
2008	29	6	#				19	13			17		#	#	#		#		54	8	#
2007	23	16	#	#	#		11	7			9		#		#				49	#	
2006	22	8					14	7			#			#	#			#	53	5	

Interesujące statystyki dotyczące liczby sądzonych, skazań i warunkowych umorzeń znajdują się też w odpowiedzi sekretarza stanu w Ministerstwie Sprawiedliwości na interpelację nr 15805 w sprawie internetowych przestępstw komputerowych[280]. Co ciekawe, dane ukryte z powodu tajemnicy statystycznej w statystykach ministerstwa, w odpowiedzi na interpelacje są podane jawnie (zob. Tabela 4).

[279] Źródło: http://bip.ms.gov.pl/pl/dzialalnosc/statystyki. Zgodnie z informacją zamieszczoną na stronie: „Znak # oznacza, że dane nie mogą być opublikowane ze względu na konieczność zachowania tajemnicy statystycznej w rozumieniu ustawy o statystyce publicznej".

[280] Dostępne na: http://orka2.sejm.gov.pl/IZ6.nsf/main/7B767D38.

Tabela 4. Dane o liczbie prawomocnych skazań osób dorosłych za przestępstwa komputerowe – czyn główny[281].

Rodzaje przestępstw przeciwko	Ogółem osądzeni	Skazani					Warunkowe umorzenie
		Ogółem skazani	Grzywna samo-istna	Ogranicz-enie wolności	Pozbawienie wolności	Środki karne	
2006							
Ogółem, w tym:	487 885	462 937	88 407	57 918	315 074	1 410	23 044
art. 267 § 1 KK	32	22	7	4	5	0	8
art. 267 § 2 KK	9	8	0	1	0	0	1
art. 267 § 3 KK w zw. z § 1	3	13	2	0	0	0	3
art. 268 § 1 KK	19	14	3	0	12	0	5
art. 268 § 2 KK	8	7	0	0	3	1	1
art. 268 § 3 KK w zw. z § 1	1	1	0	0	1	0	0
art. 268a § 1 KK	3	3	0	0	3	0	0
art. 269 § 2 KK	1	1	0	0	1	0	0
art. 269a KK	2	1	0	0	1	0	1
art. 269b § 1 KK w zw. z art. 269a KK	1	1	0	0	1	0	0
2007							
Ogółem, w tym:	449 103	426 377	82 988	47 091	294 826	1 393	20 915
art. 267 § 1 KK	32	23	8	3	10	2	9
art. 267 § 2 KK	20	16	3	4	9	0	4
art. 267 § 3 KK	3	1	0	0	1	0	2
art. 268 § 3 KK w zw. z § 1	6	3	0	1	1	1	1
art. 268 § 1 KK	13	11	1	3	7	0	2
art. 268 § 2 KK	9	7	3	0	4	0	2
art. 268 § 3 KK	1	0	0	0	0	0	1
art. 268a § 1 KK	11	9	3	1	4	1	2
art. 269 §1 KK	3	3	0	0	3	0	0
art. 269a KK	3	2	0	0	2	0	0
2008							
Ogółem, w tym:	445 204	420 729	89 011	40 643	289 269	1 686	22 587
art. 267 § 1 KK	41	29	19	2	7	1	11
art. 267 § 2 KK	6	6	3	0	3	0	0
art. 267 § 3 KK	1	1	1	0	0	0	0
art. 267 § 3 KK w zw. z § 1	2	0	0	0	0	0	2
art. 268 § 1 KK	21	19	3	1	15	0	2
art. 268 § 2 KK	15	13	6	1	6	0	2
art. 268a § 1 KK	20	17	4	1	12	0	3
art. 269 § 1 KK	1	1	0	0	1	0	0
art. 269 § 2 KK	2	2	0	0	2	0	0
art. 269a KK	1	1	0	0	1	0	0
art. 269b § 1 KK w zw. z art. 268a § 1 KK	1	1	0	0	1	0	0

[281] Źródło: http://orka2.sejm.gov.pl/IZ6.nsf/main/7B767D38.

4.3 Nielegalny dostęp do danych. Art. 267 § 1 i § 3 KK[282]

Przestępstwo uzyskiwania informacji[283] nieprzeznaczonej dla uzyskującego nazywane jest w publikacjach prawniczych przestępstwem hakingu[284] (co jest z technicznego punktu widzenia pewnym nadużyciem[285]). Ustawowe znamiona czynów zabronionych stypizowanych w paragrafach 1 oraz 3 obejmują cały szereg zachowań, spośród których tylko część ma odniesienie do informatyki i zasługuje na miano przestępstw komputerowych (trudno bowiem do takich zaliczyć odczytywanie zamkniętego listu, nieuprawnione zakładanie podsłuchów, czy przechwytywanie i deszyfrowanie kodowanych transmisji radiowych).

Pierwszym zarzutem, jaki można mieć pod adresem ustawodawcy jest więc zaniechanie wyodrębnienia w ramach osobnych przepisów przestępstw *stricte* komputerowych, co zapewne pozwoliłoby uniknąć późniejszych kłopotów z subsumpcją i wykładnią.

---

[282] Wykorzystano fragmenty artykułu: M. Szmit, I. Politowska: *O artykule 267…*, op. cit.

[283] Warto zwrócić uwagę, że użycie rzeczownika „informacji" może być interpretowane w kontekście wspomnianego wcześniej infologicznego rozumienia tego terminu. Według Macieja Siwickiego „Dla realizacji znamion art. 267 § 1 KK konieczne jest podłączenie się przez sprawcę do sieci telekomunikacyjnej (nadawca informacji będącej przedmiotem ataku musi wykorzystywać sieć przewodową, fale radiowe, optyczne lub inne środki wykorzystujące energię elektromagnetyczną). Nie stanowi przestępstwa z art. 267 § 1 KK np. podłączenie się do pojedynczego systemu komputerowego" (M. Siwicki: *Cyberprzestępczość*, C.H. Beck, Warszawa 2013, s. 113). Takie rozumienie może być słuszne, tylko wtedy gdyby przyjąć, że informacja to jedynie treść komunikatu i że penalizowane jest jedynie uzyskiwanie tej treści podczas jej transmisji, co wydaje się dość daleko idącą interpretacją.

[284] Zob. np.: P. Janas: *Przestępstwo hackingu*, „Prokuratura i Prawo" Nr 10/2009, s. 27–34.

[285] Słowo *hacker* oznacza entuzjastę komputerów. W [RFC 2828] jest ono zdefiniowane jako „(I) Someone with a strong interest in computers, who enjoys learning about them and experimenting with them. (See: cracker.) (C) The recommended definition is the original meaning of the term (circa 1960), which then had a neutral or positive connotation of »someone who figures things out and makes something cool happen«. Today, the term is frequently misused, especially by journalists, to have the pejorative meaning of cracker". Nawet pejoratywne określenie *cracke*r (definiowane w tym samym dokumencie jako „(I) Someone who tries to break the security of, and gain access to, someone else's system without being invited to do so".) obejmuje zatem nieco szerszy zakres pojęciowy, niż tylko uzyskiwanie informacji poprzez przełamywanie czy omijanie zabezpieczeń.

Pierwotna redakcja **art. 267 KK** (od 9 września 1998 r.) brzmiała:

§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

W roku 2008 przeprowadzono nowelizację KK w celu zaimplementowania Decyzji Ramowej Rady Europy 2005/222/WSiSW z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (dalej DRASI). Po nowelizacji, od 18 grudnia 2008 r. artykuł ten brzmi jak w tabeli (zob. Tabela 1).

Zmiany w redakcji pierwszego paragrafu polegały więc na:

1. zastąpieniu znamienia przestępstwa uzyskania informacji – uzyskaniem dostępu do niej;
2. zastąpienie pojęcia „przewodu" pojęciem sieci telekomunikacyjnej;
3. dodania do zabezpieczeń, zabezpieczenia informatycznego;
4. rozszerzenia ustawowego znamienia czynu zabronionego z „przełamywania" w redakcji pierwotnej do „przełamywania lub omijania" w wersji po nowelizacji.

Odpowiednio poszczególne zmiany miały na celu:

Ad 1): Uniknięcie wątpliwości odnośnie do ewentualnej konieczności udowodnienia, że sprawca czynu zapoznał się z informacją (jeśli przez „uzyskać" rozumieć – za słownikiem – „osiągnąć, otrzymać, zdobyć", to niekonieczne dla przypisania winy byłoby zapoznanie się sprawcy z informacją, do której dostęp uzyskał. Z drugiej strony

w doktrynie rozpowszechniona była[286] druga interpretacja znamienia ustawowego „uzyskiwać" (przedwojenna wykładnia Stefana Glasera i Aleksandra Mogilnickiego dokonana na gruncie art. 253 § 1 KK z 1932 r.), w której przez „uzyskanie" rozumie się zapoznanie się z treścią danej wiadomości. Stąd powstawała konieczność wykazania, że sprawca nie tylko przełamał zabezpieczenia, uzyskał dostęp do informacji, ale też, że zapoznał się z jej treścią. Ten ostatni element był w praktyce bardzo trudny do udowodnienia. Zmiana zatem miała na celu ułatwienie ścigania.

Ad 2): Rozszerzenie ochrony również na sieci bezprzewodowe. Przy okazji pojawiła się wątpliwość, czy penalizacja objęła zjawiska *warchalkingu* i *wardrivingu*[287]. Gdyby opierać się na wykładni słownikowej można by ewentualnie uznać, że już samo odebranie sygnału sieci bezprzewodowej jest jakąś formą „podłączenia się" do niej[288],

[286] Zob. np.: A. Adamski: *Prawo*..., op. cit., s. 46 i nast.; B. Fischer*: Przestępstwa*…, op. cit., s. 192; M. Karolewski: *Przestępstwa*…, op. cit.; M. Płachta: *Opinia w sprawie projektu ustawy o zmianie Kodeksu karnego, Kodeksu postępowania karnego oraz Kodeksu wykroczeń*, druk sejmowy nr 2031, Gdańsk 2004, http://orka.sejm.gov.pl/rexdomk4.nsf/(%24All)/4FC60869D85A3A73C1256E0B0047EE25/%24File/I2677-03b.rtf.

[287] *Warchalking* to oznaczanie (przez osoby postronne, skanujące sieci) miejsc, w których dostępne są sieci bezprzewodowe. Samo słowo to pochodzi z języka angielskiego (***W****ireless* ***A****ccess* ***R****evolution* – Rewolucja bezprzewodowego dostępu, *chalk* – kreda). Oznaczanie odbywa się za pomocą specjalnych symboli, które rysowane są kredą na murach. Samo zbieranie informacji na temat dostępnych sieci bezprzewodowych znane jest jako *wardriving*.

[288] Zob. np.: K. Gienias: *Odpowiedzialność prawna a ochrona sieci WLAN*, „Computerworld" z 9 lutego 2009 r., http://www.computerworld.pl/artykuly/336381/Odpowiedzialnosc.prawna.aochrona.sieci.WLAN.html; A. Adamski: *Opinia do projektu ustawy z druku nr 458: Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, Biuro Analiz Sejmowych, Toruń 4 lipca 2008 r., http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf. Na przeciwnym stanowisku – nawet odnośnie do starej redakcji omawianego paragrafu stoją autorzy artykułu M. Kliś, T. Martiszek: *Przestępstwa elektroniczne*, http://prawo.vagla.pl/skrypts/cybercrime1.htm: „Nie wydaje się uprawnione twierdzenie, że przestępstwo z art. 267 § 1 KK jest dokonane już z chwilą podłączenia się sprawcy do sieci komputerowej. Podłączenie się do przewodu służącego do przekazywania informacji jest w przypadku sieci teleinformatycznych warunkiem koniecznym do uzyskania jakiejkolwiek informacji. Nie można więc uznać go za szczególne zabezpieczenie, o którym mowa w art. 267 § 1 KK". Por. M. Kliś: *Przestępczość w Internecie*, „Czasopismo prawa karnego i nauk penalnych" Nr 1/2000.

można również mieć wątpliwości odnośnie do możliwości popełnienia w ten sposób przestępstwa stypizowanego w paragrafie 2 tegoż artykułu[289]. Na marginesie warto zauważyć, że wyrażenie „podłączając się do przewodu" czy „sieci", szczególnie w zestawieniu z „urządzeniami", o których mowa w paragrafie 3 ma wydźwięk niezamierzenie humorystyczny, współcześnie bowiem korzysta się z sieci i przewodów zawsze za pośrednictwem jakichś urządzeń.

Ad 3): Być może ustawodawcy chodziło o rozwianie ewentualnych wątpliwości, czy przełamanie zabezpieczeń informatycznych również powinno być penalizowane, jednak wobec użytego w obu redakcjach niezamkniętego katalogu zabezpieczeń („albo inne" w redakcji pierwotnej, „lub inne" po nowelizacji), takie uzupełnienie wydaje się zbyteczne.

Ad 4): Rozszerzenie ustawowego znamienia czynu zabronionego o „omijanie zabezpieczeń" było skutkiem postulatów[290] zgłaszanych m.in. przez Andrzeja Adamskiego [291] i miało doprowadzić do „uszczelnienia" karnoprawnej ochrony tajemnicy korespondencji

[289] Wątpliwości budzi zresztą sama konstrukcja art. 267 KK, który łączy w sobie dwa różne przestępstwa: nielegalny dostęp (artykuł 2 Konwencji o cyberprzestępczości) i nielegalne przechwytywanie informacji (artykuł 3 tejże konwencji). Znacznie bardziej czytelna byłaby typizacja obu czynów zabronionych w osobnych artykułach Kodeksu karnego. Por. np. P. Siemkowicz: *Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym z uwzględnieniem aktualnych zmian nowelizacyjnych*, e-biuletyn CBKE, Wrocław 2009, http://www.bibliotekacyfrowa.pl/Content/34363/Przestepstwa_skierowane.pdf; A. Adamski: *Opinia…,* op. cit.

[290] W artykule P. Siemkowicz: *Przestępstwa*…, op. cit. omówiono różne modele kryminalizacji działań „hackerskich" w tym koncepcję „naruszenia miru komputerowego", która – jak się zdaje – znalazła w tym fragmencie nowelizacji swoje odbicie.

[291] Zob. A. Adamski, *Prawo...*, op. cit., s. 51 i nast.; A. Adamski: *Opinia*…, op. cit.; M. Karolewski: *Przestępstwa przeciwko ochronie informacji w Kodeksie Karnym z 1997 r. ze szczególnym uwzględnieniem art. 267 § 1 jako przepisu kryminalizującego hacking na tle unormowań Rady Europy*, praca magisterska napisana w Zakładzie Prawa Karnego Porównawczego pod kierunkiem Anny Walczak Żochowskiej, Warszawa 2005, http://prawo.vagla.pl/files/mgr_m_karolewski.pdf; W. Wróbel [w:] *Kodeks karny. Część szczególna. Komentarz*, T. II, pod red. A. Zolla, Zakamycze 2006, s. 1311–1314.

w warunkach komunikacji elektronicznej[292]. Sam Adamski[293] rozróżnia „przełamanie" zabezpieczeń od ich „obejścia", przy czym uznaje za „obejście" takie działanie, które „nie oddziaływuje bezpośrednio na istniejące zabezpieczenia i nie usuwa ich", a jako przykłady tak rozumianych „obejść" podaje „przechwytywanie sesji (ang. *session hijacking*) i fragmentację-reasemblację pakietów" powołując się na książkę Larsa Klandera *Hacker proof*[294].

Z punktu widzenia biegłego, takie „uszczelnienie" musi budzić szereg wątpliwości. Choć – jak już wspomniano wcześniej – nie jest rolą biegłego wyrokowanie o stanie faktycznym i prawnym, łatwo można sobie wyobrazić sytuację, w której sąd zapragnie uzyskać informację o tym, na czym polegały działania oskarżonego, aby na tej podstawie móc wnioskować, czy doszło do owego przełamania lub ominięcia: dwa znamiona czynu zabronionego – wymagają od organu procesowego umiejętności rozróżnienia różnych technik penetracji i zaklasyfikowania ich do którejś z wyodrębnionych kategorii (przełamywanie/ominięcie). Nie można bowiem wykluczyć, że da się uzyskać dostęp do informacji jeszcze jakąś inną drogą. Gdyby ustawodawca uznał, że każdy sposób dostępu do informacji nieprzeznaczonej dla sprawcy winien być penalizowany, to nie musiałby szczegółowo precyzować czasownikowych znamion czynu zabronionego. Znormalizowana terminologia informatyczna nie zna jednak rozróżniania obejścia i przełamania zabezpieczeń. Definicja zawarta w Polskiej Normie brzmi: „Włamanie przełamanie – takie obejście lub zneutralizowanie jakiegoś elementu bezpieczeństwa systemu informatycznego, wykryte lub nie, którego skutkiem może być penetracja systemu przetwarzania danych"[295]. Podobnie nie rozróżniają go inne autorskie klasyfikacje ataków na systemy informatyczne[296]. Trudno spodzie-

[292] Za: A. Adamski: *Opinia…*, op. cit.

[293] A. Adamski: *Prawo...*, op. cit., s. 51 i nast.

[294] L. Klander: Hacker *Proof: The Ultimate Guide to Network Security*, Jamsa Pr., 1997; edycja polska L. Klander: *Hacker proof, czyli jak się bronić przed intruzami*, Mikom, Warszawa 1997.

[295] W wersji anglojęzycznej: „Breach – The Circumvention or disablement of some element of computer security, with or without detection, which could result in a penentration of the data processing system". Zob. PN-ISO/IEC 2382-8:2001-08.05.17.

[296] Przykładowe klasyfikacje zostały omówione w artykule M. Szmit, I. Politowska: *O artykule 267…*, op. cit.

wać się, żeby biegły informatyk znał wykładnię operatywną i wyjaśniał sądowi ewentualne wątpliwości zgodnie z nią – pomijając obowiązujące w jego dziedzinie wiedzy normy. Byłoby to zresztą sprzeczne zarówno z zasadami opiniowania, jak i ze zdrowym rozsądkiem. W powołanej książce autor używa określenie obejścia: „nie oddziaływuje bezpośrednio na istniejące zabezpieczenia i nie usuwa ich", jak więc można się domyślać, przełamanie powinno oddziaływać bezpośrednio na istniejące zabezpieczenia lub usuwać je. O ile usuwanie zabezpieczeń jest przypadkiem dość oczywistym, o tyle pojęcie „bezpośredniego oddziaływania na zabezpieczenia" może budzić szereg wątpliwości. Zapewne właściwe byłoby tu mówienie o jakimś oddziaływaniu na mechanizm zabezpieczający, powodującym jego działanie niezgodne z intencją twórcy, tyle że takim działaniem byłby i – na przykład – atak typu SQL-injection, który trudno uznać za coś innego, niż wykorzystanie luki w bardzo źle napisanym zabezpieczeniu systemu[297].

[297] Ciekawy przypadek karnoprawnej kwalifikacji takiego ataku miał miejsce w postępowaniu przed Sądem Rejonowym w Głogowie. Sąd (pod rządami przepisu w jego brzmieniu sprzed nowelizacji) uniewinnił prawomocnie oskarżonego o czyn z art. 267 par 1 KK, który posłużył się techniką SQL-injection wykorzystując w ten sposób lukę w istniejących zabezpieczeniach. Sąd w uzasadnieniu wyroku napisał m.in.: „Zdaniem Sądu, mając na uwadze obecną treść art. 267 § 1 KK, ustawodawcy chodzi o przełamanie istniejącego zabezpieczenia. Nie można przełamać czegoś, co nie istnieje. Za taką interpretacją przemawia chociażby słownikowa definicja bezokolicznika »przełamywać« jako »łamanie czegoś, przezwyciężanie czegoś, zwalczanie czegoś« (*Popularny słownik języka polskiego*, Wydawnictwo Wilga, Warszawa 2000)", później jednak odniósł się do (podówczas znajdującej się jeszcze na etapie projektu) nowelizacji rozszerzającej znamiona czynu zabronionego o „omijanie" pisząc: „Zupełnie czymś innym jest ominięcie zabezpieczenia poprzez znalezienie w nim luki. Za takim wnioskiem przemawia powołany proponowany projekt zmiany 267 § 1 KK, gdzie rozszerza się katalog czasownikowych zachowań sprawcy również i o ominięcie elektronicznego zabezpieczenia". Zob. P. Waglowski: *Nie można przełamać czegoś, co nie istnieje polski wyrok w sprawie SQL Injection*, http://prawo.vagla.pl/node/8154. Do drugiej części uzasadnienia można mieć wątpliwości, rzeczy i zjawiska nieistniejące równie trudno bowiem przełamywać jak i obchodzić. Ciekawe rozważania na ten temat zawiera artykuł A. Baworowskiego, który postuluje, że aby mówić o zabezpieczeniach muszą one mieć charakter zupełny, przynajmniej na poziomie podstawowym (jeśli dysponent pozostawi możliwości nieuprawnionego dotarcia do informacji, nie wprowadzając co najmniej zabezpieczeń producenta, to nie można mówić o zabezpieczeniu). Za ominięcie należałoby więc, w takiej interpretacji, uznać znalezienie i wykorzystania nowej (nieznanej przez producenta) luki w zabezpieczeniach. Zob. A. Baworowski: *Problemy wykładni przepisów art. 268 § 2, 269 § 2 i 269a KK po nowelizacjach z 2008 r.*, „Diariusz Prawniczy" Nr 10/11/2009.

Przy okazji dyskusji o przełamaniu" i „ominięciu" widać – zapewne podświadome – traktowanie przez prawników i prawodawcę zabezpieczeń informatycznych analogicznie do zamknięcia pomieszczenia fizycznego i do włamania doń[298]. Tymczasem z punktu widzenia bezpieczeństwa informacji zabezpieczenia nie ograniczają się do zabezpieczeń fizycznych, definiuje się je jako „środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządcą lub prawną"[299]. Jako przykłady zabezpieczeń w systemach informatycznych podaje się choćby: mechanizmy kontroli dostępu, oprogramowanie antywirusowe,

[298] W tym kontekście należy przywołać:

- ✓ wypowiedź Sądu Najwyższego w wyroku z 24 czerwca 1958 r. (IV KRN 170/58) „Podstawową istotą włamania jest wtargnięcie sprawcy do zamkniętego pomieszczenia, przez usunięcie przy użyciu siły fizycznej przeszkody zamykającej dostęp do danego pomieszczenia. Pomieszczenie musi być zamknięte, tj. w taki sposób zabezpieczone przed wtargnięciem osób powołanych by normalne wejście było niemożliwe. Usunięcie takiej przeszkody jest wyraźnym obejściem woli właściciela pomieszczenia niedopuszczenia osoby trzeciej do tegoż pomieszczenia. Zaznaczyć tu należy, iż wola ta musi być w poważny sposób wyrażona. Zamknięcie pomieszczenia na zwykły haczyk, który bez większej trudności każdy może odsunąć, czy też zwykłą klamkę bez użycia klucza nie może być traktowane jako zamknięcie pomieszczenia i w takich wypadkach wejścia doń sprawcy i dokonanie kradzieży nie można traktować jako włamania";
- ✓ uchwałę całego składu Sądu Najwyższego z 25 czerwca 1980 r. (VII KZP 48/78), w której Sąd Najwyższy stwierdził: „Za pomieszczenie zamknięte można uznać między innymi: wszelkiego rodzaju budynki, skarbce, schowki (np. Kasy pancerne, kasetki, szafy, biurka), specjalne środki transportu (np. kolejowe wagony, samochody: chłodnie, cysterny, warsztaty) i inne środki służące do transportu ludzi lub mienia oraz wszelkiego rodzaju zbiorniki i pojemniki służące do przechowywania, przekazywania lub przesyłania mienia do obrotu towarowego, transportu. Warunkiem uznania któregokolwiek z wymienionych przykładowo pomieszczeń za zamknięte, tj. za takie, które może być obiektem włamania w rozumieniu art. 208 KK, jest ustalenie nie tylko okoliczności, że powierzchnię zamkniętą tworzy jego zwykła konstrukcja, ale również i okoliczność, że jego otwory poza zwykłym zamknięciem (np. zamknięcie drzwi na zwykłą klamkę, haczyk, zewnętrzną zasuwkę; zbiornika lub pojemnika zwykłą pokrywą) były zaopatrzone w specjalne przeszkody materialne (zamknięcie) utrudniające dostęp do wnętrza pomieszczenia. Takimi przeszkodami materialnymi mogą być w zależności od konstrukcji, rodzaju lub przeznaczenia pomieszczenia – np. różnego rodzaju kłódki, czy plomby".

[299] PN-ISO/IEC 17799:2007-2.2.

szyfrowanie w celu uzyskania poufności, podpisy cyfrowe, zapory sieciowe, zasilanie rezerwowe czy kopie zapasowe[300]. W przypadku zabezpieczeń natury informatycznej czy organizacyjnej trudno jest mówić o usunięciu przeszkody przy użyciu siły fizycznej, stąd trudności w ustaleniu, czy dochodzi do jej przełamania. Z drugiej strony trudno sobie wyobrazić penalizację skorzystania z innego niż przewidziany przez producenta bądź administratora systemu sposobu dostępu do zgromadzonych w dowolnym systemie danych. Dla przykładu: część serwisów www utrzymujących się z wyświetlania płatnych reklam używa jako zabezpieczenia (z technicznego punktu widzenia, zabezpieczenia wybitnie niskiej jakości) mechanizmu tzw. ukrytych stron (stron ukrytych pod trudnymi do odgadnięcia adresami URL[301]) wymuszającego konieczność odwiedzania stron w narzuconej kolejności. Internauci podejmują czasem próby odgadnięcia adresów takich stron, a zatem, co najwyżej obejścia – bo przecież nie „przełamania" – takiego zabezpieczenia. W praktyce takiego działania nie można odróżnić od kilkukrotnej pomyłki przy wpisywaniu znanego adresu URL (chyba że kolejne adresy będą generowane przy użyciu programu, który sprawdzi tysiące czy dziesiątki tysięcy adresów URL). Karalność takiego zachowania byłaby więc co najmniej wysoce problematyczna[302].

Do ujawniania ukrytych stron dochodzi czasem poprzez działanie wyszukiwarek, należałoby więc rozstrzygnąć, czy karać twórców robotów, czy może osoby, które zamieszczając nieodpowiednie informacje umożliwiły robotowi trafienie na ukryte strony. Z problematyką robotów webowych związana jest też inna kwestia: przeszukiwanie „ukrytych zasobów" (jak również

[300] Zob. PN-I-13335-1:1999- 8.6.

[301] Jest to jedna z form tzw. ukrytego Internetu. Por. np. N. Pamuła-Cieślak: *Zjawisko Ukrytego Internetu – rola bibliotek w upowszechnianiu jego zasobów*, Materiały II Konferencji Biblioteki Politechniki Łódzkiej: *Biblioteki XXI wieku. Czy przetrwamy?*, s. 379–386, Łódź 2006, http://eprints.rclis.org/8925/1/pamula.pdf; A. Strzelecki: *Legal Aspects of Deep Links on the Internet, Proceedings of the International Multiconference on Computer Science and Information Technology*, s. 559–563.

[302] Stosunkowo głośny był przypadek ujawniania takich danych należących do banku PKO BP w 2010 r. Osoba, która odkryła możliwość dostępu do danych bankowych poinformowała o tym bank, który z kolei złożył doniesienie do prokuratury. Sprawa skończyła się umorzeniem śledztwa przez prokuraturę. Zob. np.: P. Konieczny: *„Głębokie ukrycie" danych w PKO BP*, http://niebezpiecznik.pl/post/glebokie-ukrycie-danych-w-pko-bp.

wykorzystywanie innych luk w serwisach www) można realizować w zawoalowanej formie – przy użyciu robotów webowych[303] umieszczając po prostu na specjalnie napisanej stronie odpowiednio spreparowane odsyłacze. W takim wypadku „sprawcą" jest robot webowy, który podążając za odsyłaczami wchodzi w interakcje ze (źle zabezpieczonym) serwisem www. Powodowałoby to dalsze problemy z przypisaniem odpowiedzialności za takie „przełamanie lub omijanie zabezpieczeń".

Niezależnie od powyższego samą praktykę „uszczelniania" czy rozszerzania przepisów poprzez leksykalne zabiegi dodawania kolejnych czasowników, o nie do końca jasnym znaczeniu do ustawowych znamion czynów zabronionych, należy ocenić negatywnie. Tego rodzaju kazuistyczny sposób formułowania przepisów, przynajmniej w tak szybko rozwijającej się dziedzinie jak prawo komputerowe, prowadzi do powstania prawa niezrozumiałego i trudnego do stosowania.

Zmiany w redakcji paragrafu trzeciego (przed nowelizacją KK – drugiego) polegały na dodaniu do ustawowego znamienia czynu zabronionego możliwości penalizacji posługiwania się oprogramowaniem[304], przy czym pierwotna rządowa propozycja nowelizacji zawierała określenie „specjalnym", słowo „specjalnym" zostało wykreślone po procesie konsultacji społecznych[305]. W efekcie powstał przepis wybitnie nieczytelny i trudny w stosowaniu, bowiem po pierwsze w odróżnieniu od paragrafu pierwszego tego samego artykułu, pozostawiono w artykule trzecim pojęcie „uzyskania informacji", a nie dostępu do niej. O ile więc osiągnięcie skutku w postaci uzyskania dostępu do informacji będzie penalizowane, to sama próba jego osiągnięcia pozostanie raczej bezkarna (chyba że – zgodnie z tym, co napisano powyżej – dałoby się osobie próbującej przełamać zabezpieczenia udowodnić, że czyni to w celu zapoznania się z informacją, a nie tylko uzyskania do niej dostępu[306], co jest oczywiście w praktyce bardzo trudne, bądź – że

[303] Zob. np.: M. Zalewski: *Cisza w sieci. Praktyczny przewodnik po pasywnym rozpoznawaniu i atakach pośrednich*, Helion, Gliwice 2005, s. 121.

[304] Ewentualne wątpliwości budziło, czy komputer z zainstalowanym na nim oprogramowaniem do *sniffingu* (podsłuchu) sieci może być klasyfikowany jako urządzenie specjalne. Zob. np.: A. Bojańczyk: *Karnoprawne aspekty ochrony prawa pracownika do tajemnicy komunikowania się* (Część II), „Palestra" Nr 3/2003, http://www.palestra.pl/index.php?go=artykul&id=941.

[305] Zob. http://orka.sejm.gov.pl/proc6.nsf/projekty/458_p.htm.

[306] Por. np. P. Siemkowicz: *Przestępstwa*…, op. cit.

sąd zechce użyć innej wykładni tego pojęcia). Po wtóre usunięcie słowa „specjalnym" rozszerzyło znamiona czynu na dowolny sprzęt i oprogramowanie, co – przynajmniej przy słownikowym rozumieniu przepisu – prowadzić musi do absurdalnych sytuacji. Również uzasadnienia zapadłych w przeszłości wyroków dotyczące posługiwania się standardowymi urządzeniami[307], przy nowej redakcji przepisu musiałyby być inne. Wydaje się, że przez usunięcie słowa „specjalne" ustawodawca spowodował daleko idącą nadkryminalizację; z formalnego punktu widzenia bowiem znamiona czynu zabronionego wypełniała np. osoba wchodząca za pomocą przeglądarki internetowej w sieci www na strony opatrzone ostrzeżeniem np. „tylko dla osób powyżej 21 roku życia" (o ile sama nie ma ukończonych 21 lat). Wątpliwa jest również sytuacja różnego rodzaju hobbystów korzystających ze standardowych urządzeń odbiorczych do nasłuchiwania transmisji lotniczych, kolejowych, komunikatów służb ratunkowych, taksówkarzy, czy nawet krótkofalowców, o ile ci rozmawiają ze sobą nawzajem. Wydaje się, że w tym przypadku można jeszcze argumentować, że trudno uznać radioodbiornik za urządzenie podsłuchowe, ale nie da się tej argumentacji zastosować do „urządzeń wizualnych" czy „oprogramowania"[308]. Sytuację pogarsza fakt, że – w przeciwieństwie do zapisów paragrafu pierwszego powołanego artykułu – przestępstwo stypizowane w paragrafie trzecim nie wymaga już nie tylko przełamywania, czy omijania jakichkolwiek zabezpieczeń, ale nawet ich istnienia.

[307] Por. np. wyrok Sądu Najwyższego z 19 października 2006 r. (V KK 221/06), w którym sąd m.in. stwierdził: „1. Urządzenie nadawczo-odbiorcze Alan CT 145 nie jest urządzeniem specjalnym w rozumieniu art. 267 § 2 KK […]". Zob. też: P. Waglowski: *Wyrok za słuchanie*, http://prawo.vagla.pl/node/5039.

[308] Nie sposób zgodzić się więc np. z argumentacją P. Siemkowicza (*Przestępstwa…*, op. cit.), w myśl której „Zmiana na gruncie nowelizacji z 24 października 2008 r., sprowadzała się przy tym jedynie do zamiany zwrotu »posługiwania się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym« na sformułowanie »posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem«. Oczywistym jest przy tym, że pomimo tego, iż sam program komputerowy nie jest urządzeniem, to już komputer z zainstalowanym właściwym programem (np. typu *password sniffer*) pozwalającym na monitorowanie ruchu w sieci i przechwytywanie początkowych sekwencji bajtów danej sesji zawierającej identyfikatory i hasła dostępu, będzie urządzeniem o charakterze specjalnym (…). Tym samym wskazana zmiana legislacyjna miała jak się wydaje charakter jedynie kosmetyczny".

Na marginesie można wspomnieć jeszcze o dodatkowej trudności, jaką powoduje kwalifikacja prawna czynów, których znamiona są podobne do ustawowych znamion czynu zabronionego omawianego artykułu, w szczególności nielegalnego odbioru sygnału telewizyjnego oraz nielegalnego współdzielenia sygnału telewizyjnego (tzw. przestępstwo *sharingu*), który podlega ściganiu – wbrew temu, czego można by się spodziewać – z art. 6 oraz 7 UONUŚDE[309].

[309] Zob. np.: wyrok Sądu Najwyższego z 24 marca 2004 r. (IV KK 46/04). Sąd stwierdził: „Istotą występku, o jakim mowa w art. 267 § 1 KK jest uzyskanie informacji dyskrecjonalnej, nie przeznaczonej dla sprawcy. Program emitowany w sieci kablowej z natury rzeczy przeznaczony jest dla każdego, kto tylko uiści abonament. Tak więc informacje zawarte w tym programie nie są informacjami, które nie są przeznaczone dla potencjalnych odbiorców. Sprawca, który bezprawnie z takich programów korzysta i pozyskuje zawarte w nich informacje, nie narusza więc dyspozycji art. 267 § 1 KK, lecz godzi jedynie w prawa majątkowe". To stanowisko Sądu Najwyższego było krytykowane w doktrynie (por. S. Hoc: *Karnoprawna ochrona informacji*, Uniwersytet Opolski, Opole 2009, s. 81 i nast.).
Zob. też. postanowienie Sądu Najwyższego z 29 września 2004 r. (I KZP 21/04), w którym sąd m.in. stwierdził: „(…) Charakterystyczne jest, że Sąd Okręgowy, koncentrując się na eksponowaniu różnic między wymienionymi w art. 121 § 2 KW, podlegającymi wyłudzeniu świadczeniami a opisywaną usługą telekomunikacyjną operuje, niejako automatycznie, pojęciem »wyłudzenia odbioru sygnału telewizyjnego«. Poprzestaje na tym jednak i z faktu tego nie wyciąga żadnych wniosków. Tymczasem uznanie opisanego zachowania za wyłudzenie w połączeniu ze stwierdzeniem, iż działanie to godzi w prawa majątkowe przedsiębiorstwa będącego nadawcą programu, powinno kierować jego ocenę na tory norm sankcjonowanych, określających uzyskanie bezprawnej korzyści przy pomocy określonych zabiegów i wyrządzenie szkody. Należą do nich normy regulujące oszustwo (art. 286 § 1 KK), bądź szalbierstwo (art. 121 § 2 KW), z których druga posługuje się wprost znamieniem wyłudzenia świadczenia płatnego. Nie powinno budzić wątpliwości, że w pojęciu wyłudzenia – dla zrealizowania zamiaru uniknięcia zapłaty należności za uzyskiwane świadczenie – mieści się działanie podstępne, które może polegać zarówno na wprowadzeniu kogoś w błąd, na wyzyskaniu jego błędu, jak i przede wszystkim, co godne podkreślenia, na bezpośrednim wyzyskaniu wytworzonej podstępnie sytuacji (wyzyskaniu nieświadomości). Takie rozumienie wskazanego wyrażenia ustawowego obowiązywało już na gruncie, stanowiącego odpowiednik art. 121 § 2 KW, przepisu art. 265 KK z 1932 r., którego komentatorzy (por. m.in. L. Peiper: *Komentarz do Kodeksu karnego*, Kraków 1933, s. 745; J. Makarewicz: *Kodeks karny z komentarzem*, Lwów 1935, s. 464; W. Makowski: *Kodeks karny, komentarz*, Warszawa 1937, s. 812–813) wskazywali na brak zasadniczych różnic w istocie szalbierstwa i oszustwa, zaś odmienności upatrywali m.in. właśnie w sposobie działania polegającego na wyzyskaniu nieświadomości, jakie to działanie, inaczej niż wprowadzenie w błąd lub wyzyskanie błędu, nie mieści się w znamionach oszustwa. Poglądy te, zaaprobowane w judykaturze Sądu Najwyższego (por. m.in. uzasadnienie uchwały z 29 lipca 1971 r. (IV KZP 17/71), zachowały aktualność w obecnym stanie prawnym.

Dlatego należało rozważyć, czy w ramach szalbierczego wyłudzenia, obejmującego bezpośrednie wyzyskanie wytworzonej podstępnie sytuacji, nie mieści się działanie polegające na samowolnym podłączeniu się bez wiedzy operatora do sieci kablowej w celu uzyskania świadczenia dostępu do programów bez uiszczenia należnych wówczas (za podłączenie i przekaz) opłat. Uznanie bowiem zachowania za oszustwo przy stwierdzeniu, że szalbierstwo, ze względu na sposób i przedmiot działania, jest szczególną jego postacią wymagałoby stwierdzenia, że uzyskanie, w celu osiągnięcia korzyści majątkowej, dostępu do programów nastąpiło w wyniku doprowadzenia operatora (za pomocą wprowadzenia go w błąd lub wyzyskania jego błędu) do niekorzystnego rozporządzenia mieniem. To zaś ewentualnie mogłoby mieć miejsce w wypadku zawarcia z operatorem umowy o świadczenie usług telekomunikacyjnych w celu osiągnięcia dostępu do sieci, a następnie wykorzystania tego dostępu w sposób wykraczający poza warunki tej umowy, dotyczące np. czasu lub zakresu udostępnionego podłączenia albo zakresu udostępnionych programów. Rzecz jasna, w każdej z rozważanych sytuacji kluczowe znaczenie miałby stan świadomości sprawcy w momencie podejmowanych działań. W wypadku szalbierstwa chodzi o wolę bezpłatnego skorzystania ze świadczenia przy świadomości jak wskazano w uchwale Sądu Najwyższego z 24 stycznia 1973 r., (VI KZP 69/72) – że usługa ta jest płatna tak jak świadczenia wymienione przykładowo w przepisie art. 121 § 2 KW, tzn. z reguły bezzwłocznie (...)".

Na marginesie warto zauważyć, że powyższe rozważania, dotyczące szalbierstwa, mogą mieć zastosowanie również w odniesieniu do przestępstwa nielegalnego uzyskania dostępu do systemu, tj. art. 267 § 2 KK (zob. rozdział 4.4). czy oszustwa komputerowego (zob. rozdział 4.10).

Zob. też uchwała SN z 22 stycznia 2003 r. (I KZP 43/02), w której sąd stwierdził m.in.: „Niezależnie od tego, należy podkreślić, iż istotą występku, o jakim mowa w art. 267 § 1 KK, jest uzyskanie informacji dyskrecjonalnej, nie przeznaczonej dla sprawcy. Program emitowany w sieci kablowej z natury rzeczy jest przeznaczony dla każdego, kto tylko uiści abonament. Tak więc informacje zawarte w tym programie nie są informacjami, które nie są przeznaczone dla potencjalnych odbiorców. Sprawca, który bezprawnie z takich programów korzysta i uzyskuje zawarte w nich informacje, nie narusza więc dyspozycji art. 267 § 1 KK lecz, podobnie jak głodny informacji sprawca kradzieży czasopisma, godzi jedynie w prawa majątkowe. Dysponent informacji jest władny mniej lub bardziej szeroko określić krąg podmiotów, dla których informacja jest przeznaczona. Każdy, kto spoza tego kręgu, uzyskałby takową informację, działaniem swoim wyczerpuje znamiona przestępstwa określonego w art. 267 § 1 KK. Uprawnienie do uzyskania informacji, o jakim mowa w art. 267 § 1 KK, nie może w odniesieniu do prasy drukowanej, a także przekazów radiowych i telewizyjnych sprowadzać się jedynie do konieczności wniesienia opłaty. W istocie rzeczy informacja zawarta w prasie drukowanej, przekazie radiowym i telewizyjnym ma bowiem charakter powszechny, skierowana jest do każdego. Zapłata za informację w cenie prasy drukowanej lub prawa do odbioru programu emitowanego w sieci kablowej jest wynikiem faktu, iż dostarczanie informacji stanowi specyficzną usługę. Wymogu tego nie należy łączyć i utożsamiać z uprawnieniami, których istnienia wymaga art. 267 § 1 KK".

Przy okazji można zwrócić uwagę na zagadnienie ujawnienia informacji penalizowanego w art. 267 § 4 KK. Jak się wydaje w tym wypadku ustawodawca w prawidłowy sposób użył słowa „ujawnienie". Polskie normy definiują ujawnienie (ang. *disclosure*) jako „Naruszenie

Art. 6. 1*:*

Kto, w celu użycia w obrocie, wytwarza urządzenia niedozwolone lub wprowadza je do obrotu, podlega karze pozbawienia wolności do lat 3.

2. Tej samej karze podlega, kto świadczy usługi niedozwolone.

Art. 7. 1*:*

Kto, w celu osiągnięcia korzyści majątkowej, posiada lub używa urządzenie niedozwolone, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

2. Jeżeli sprawca używa urządzenia niedozwolonego wyłącznie na własne potrzeby, podlega grzywnie.

Podsumowując: w obecnym brzmieniu artykuł 267 § 1 i § 3 KK jest konstrukcją bardzo daleką od doskonałości i trudną w praktycznym stosowaniu. Opiniowanie w sprawach dotyczących przestępstw komputerowych stypizowanych w tych paragrafach wymaga od biegłego ponadstandardowej uwagi i znajomości nie tylko swojej dyscypliny, ale i wykładni operatywnej przepisów prawa[310].

bezpieczeństwa systemu informatycznego, po którym dane mogą być dostępne dla nieuprawnionych jednostek" [PN-I-02000:2002-3.1.106], [PN-ISO/IEC 2382-8:2001-08.05.15]. Czasownik „ujawnia" jest użyty również w art. 265 i 266 KK w odniesieniu do informacji niejawnej. W szczególności zatem nie można, jak się wydaje, mówić o ujawnieniu informacji jawnej (nawet jeśli jest ona komuś nieznana; w takim przypadku można mówić co najwyżej o przekazaniu komuś informacji).

[310] W pełni należy się zgodzić z krytyczną opinią M Siwickiego: „Dokonując [...] ogólnej oceny unormowania, jakie zawiera art. 276 § 1. KK należy stwierdzić, że funkcję ochronną tego przepisu poważnie osłabia uzależnienie odpowiedzialności karnej sprawcy od tego, czy jego czyn – często sztucznie – będzie można zakwalifikować jako „przełamanie" lub „ominięcie" elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia informacji. Rozwiązanie takie nie tylko nie odpowiada współczesnym standardom normatywnym w zakresie penalizacji hakingu, w których odchodzi się od koncepcji ochrony »komputerowego domicylu«, ale jest także unikalne na tle porównawczym, anachroniczne i w praktyce niezdolne do właściwego wypełniania funkcji polityczno-kryminalnych" (M. Siwicki: *Cyberprzestępczość…*, op. cit., s. 120).

4.4 Nielegalny dostęp do systemu. Art. 267 § 2 KK

Redakcja paragrafu drugiego artykułu 267 KK wprowadzonego doń w ramach nowelizacji KK w 2008 r. (zob. Tabela 1) jest – podobnie jak omówiony wyżej sposób typizacji przestępstwa nielegalnego przechwytywania danych – przykładem niechlujstwa ustawodawcy. Wspomniane wcześniej umieszczenie w obrębie jednego artykułu znamion dwóch różnych czynów przestępnych z przewagą granic stosowania przepisu uzupełniającego nad zasadniczym[311] jest tu jedynie jednym z mankamentów.

Symptomatyczne jest nieskorzystanie przez krajowego ustawodawcę z – istniejącej w KREoC – możliwości zawężenia znamion przestępstwa poprzez wymóg celu kierunkowego: „Strony mogą wprowadzić wymóg, że przestępstwo musi zostać popełnione poprzez naruszenie zabezpieczeń, z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem, lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym", które wpisuje się w tendencję nadkryminalizacji zachowań związanych z użytkowaniem technik informatycznych. W połączeniu z bardzo ogólnym ujęciem ustawowych znamion czynu zabronionego, skutkuje to bardzo szerokim zakresem czynów, które mogłyby zostać zakwalifikowane jako spełniające owe znamiona[312]. *Sensu largo* takim uzyskaniem dostępu jest przecież zarówno uzyskanie dostępu poprzez sieć komputerową (sformułowanie „w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym" w KREoC), jak i uzyskanie dostępu fizycznego, np. poprzez wejście nieuprawnionego pracownika do pomieszczenia, w którym przetwarzane są dane (np. do serwerowni), a więc czyn, który – w przytłaczającej większości przypadków[313] – będzie, co najwyżej, naruszeniem obowiązków czy uprawnień pracowniczych. Biorąc zresztą pod uwagę, że współcześnie systemy informatyczne znajdują się niemal wszędzie, można by równie dobrze uznać,

[311] Por. np. P. Siemkowicz: *Przestępstwa*…, op. cit.

[312] Por. ibid.: „Sytuacja ta stwarza (…) niebezpieczeństwo niedookreśloności omawianego przepisu z art. 267 § 2 KK, a tym samym zbyt dużej swobody jego interpretacji przez organy ścigania oraz organy procesowe".

[313] Wyjąwszy miejsca, w których przetwarzane są dane niejawne.

że osoba włamująca się[314] do samochodu uzyskuje dostęp do zamontowanych w nim (i połączonych ze sobą w sieć CAN – *Car Area Network*) urządzeń informatycznych, tworzących niewątpliwie system informatyczny, podobnie można by zaklasyfikować działanie osoby wchodzącej – bez uprawnienia – do cudzego domu (o ile znajduje się nim komputer czy komputery połączone ze sobą). Krajowy ustawodawca zrezygnował przecież z możliwości ograniczenia penalizacji uzyskiwania dostępu do systemu wyłącznie do działań podjętych w celu uzyskania dostępu do danych informatycznych (przestępstwa kierunkowego), a więc działanie w zamiarze kierunkowym nie jest konieczne.

Kolejnym problemem, jaki rodzi tak szeroka kryminalizacja jest – podnoszony w części publikacji – argument, że w praktyce każde nielegalne przechwytywanie danych przetwarzanych w systemie informatycznym będzie wiązało się z uzyskaniem nieuprawnionego dostępu do całości lub części systemu informatycznego[315], zatem czyn penalizowany w artykule 267 §1 KK, o ile dotyczył będzie informacji przesyłanej w sieci komputerowej, z konieczności będzie również wypełniał znamiona przestępstwa z art. 267 § 2 KK. Można oczywiście utrzymywać, że tym razem ustawodawca pisząc o „informacji" miał na myśli nie tylko treść komunikatu (a więc informację w procesie jej przesyłania), ale i dane zapisane na nośniku (por. przypis 277), niemniej niewątpliwie trudno uznać redakcję tego artykułu za wystarczająco czytelną i jednoznaczną.

[314] Nie jest zresztą konieczne włamanie, bowiem przestępstwo spenalizowane w omawianym artykule nie wymaga przełamywania, a nawet istnienia jakiegokolwiek zabezpieczenia.

[315] Aleksandra Suchorzewska przytacza tezę, że „wraz z rozwojem technologii wprowadzony do Kodeksu karnego nowy typ zachowania przestępnego może w przyszłości zastąpić tradycyjne przestępstwo nieuprawnionego dostępu do informacji" (A. Suchorzewska: *Ochrona…*, op. cit., s. 219). Jak się wydaje jednak ustawowe znamiona czynu zabronionego nie obejmują w tym wypadku niektórych czynności mieszczących się w schemacie działania znanym jako *elevation of privileges*, w którym osoba uprawniona do wykorzystania systemu informatycznego w jakimś zakresie, rozszerza w sposób nieuprawniony ów zakres, nie można więc mówić o sytuacji „uzyskiwania dostępu do systemu bez uprawnienia", o tyle, że wprawdzie owo rozszerzenie uprawnień nie musi skutkować możliwością uzyskania dostępu do części systemu, do której bez tego działania tego dostępu osoba ta nie miała: np. w przypadku nielegalnego podniesienia uprawnień z możliwości jedynie czytania jakiejś treści (*read-only*) do możliwości jej zapisu (*read-write*).

4.5 Naruszanie integralności danych. Art. 268 i Art. 268a KK

Czyny stypizowane w art. 268 i 268a KK (zob. Tabela 1) nazywa się w literaturze przestępstwami przeciwko integralności danych. Jest to nazwa nie do końca poprawna[316], integralność bowiem (zgodnie z tym, co napisano wcześniej) jest to własność polegająca na zapewnieniu dokładności i kompletności aktywów (w tym wypadku aktywami są zapis informacji w art. 268 KK bądź dane informatyczne w art. 268a KK). Naruszenie integralności danych w ogólności jest to nieuprawnione usunięcie jakiegoś ich fragmentu, nieuprawnione dopisanie jakichś danych dodatkowych[317], bądź nieuprawniona modyfikacja danych istniejących. W szczególności – o utracie integralności mówi się w przypadku, w którym na skutek celowego złośliwego działania czy awarii technicznej, została zaburzona spójność powiązań (relacji) pomiędzy powiązanymi ze sobą danymi. Jak można zauważyć, ustawowe znamiona czynów zabronionych, oprócz czasowników odpowiadających czynnościom prowadzącym do utraty integralności (uszkadza, usuwa, zmienia), zawierają szereg czasowników odpowiadającym czynnościom niezwiązanym z tą własnością bezpieczeństwa informacji (niszczy, usuwa, udaremnia,

[316] Jeszcze dziwniejsza jest jednak – funkcjonująca również w literaturze prawniczej – nazwa „szkody w bazach danych" (zob. np.: S. Koc: *Karnoprawna ochrona informacji*, Wydawnictwo Uniwersytetu Opolskiego, Opole 2009, s. 115) w odniesieniu do artykułu 268a KK. Można zresztą – na marginesie – odnieść wrażenie, że część prawników ma tendencję do utożsamiania „danych informatycznych" z pojęciem „baz danych". W rzeczywistości ochroną baz danych zajmuje się ustawa o ochronie baz danych (dalej UOBD), definiująca bazę danych w art. 2 ust. 1 pkt 1 jako „zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości".

[317] Warto na marginesie zauważyć, że wśród znamion czynu zabronionego pominięto czynności polegające na dodaniu czegokolwiek do atakowanego systemu. W przypadku dodania dodatkowych danych, można wprawdzie wywodzić, że dopisanie czegokolwiek do już istniejącego zapisu jest jego modyfikacją, natomiast poza zakresem karalności pozostaje w ten sposób np. wprowadzanie do cudzego systemu nieautoryzowanych zmian, polegających na zainstalowaniu oprogramowania (por. A. Adamski: *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" Nr 4/2005), trudno bowiem uznać – przy tym wszystkim, co napisano powyżej na temat rozumienia przez prawników pojęć „informacja" i „dane informatyczne", aby program komputerowy mógł być za takowe uznany.

utrudnia, zakłóca, uniemożliwia). Po części te znamiona związane są z naruszaniem dostępności[318], po części można je interpretować jako działanie przeciwko niezawodności. Pewnym problemem może być także nie najszczęśliwsze sformułowanie „utrudnia dostęp", bowiem utrudnienie komuś dostępu do informacji (danych informatycznych) nie musi być związane z działaniem przeciwko dostępności informacji w jakimś systemie, ale może dotyczyć działań podjętych wobec konkretnej osoby, np. ograniczenia jej wolności, która w konsekwencji tych działań nie będzie mogła zapoznać się z ową istotną informacją. Również pojęcie „informacji" w art. 268 KK powoduje, że może dotyczyć on nie tylko zagadnień informatycznych, ale i przestępstw przeciwko bezpieczeństwu informacji przetwarzanej w sposób klasyczny (np. spalenie papierowego listu). Wątpliwości budzi również stosunek zakresu penalizacji określonego w 286 § 2 KK do artykułu 286a KK (w literaturze podnosi się argument, że pojęcie „dane informatyczne" obejmuje również dane zapisane na informatycznym nośniku danych)[319].

Kolejną trudnością jest użyty w znamieniu czynu zabronionego w artykule 268a KK (jak również w omówionym poniżej artykule 269 KK) przymiotnik „istotny" pozostawiający dużą swobodę interpretacyjną[320]. Można

[318] Zob. ibid. Integralność jest wśród pojęć CIA pojęciem najszerszym, w tym sensie, że dowolna (poza biernym podsłuchem) nieuprawniona operacja z danymi bądź programami prowadzi do – mniejszych lub większych – zmian w takowych, a więc może być traktowana jako spowodowanie zaburzenia integralności.

[319] Zob. np.: A. Suchorzewska: *Ochrona*…, op. cit., s. 221.

[320] B. Kunicka-Michalska: *Komentarz do artykułów 222–316* [w:] A. Wąsek, R. Zawłocki: *Kodeks Karny. Część szczegółowa*, C.H. Beck, Warszawa 2010, s. 376: „Chodzi o sytuacje, gdy w ocenie przeciętnego dysponenta i użytkownika systemu komputerowego lub sieci teleinformatycznej stopień zakłócenia jest istotny, to znaczy nie taki, który da się szybko i bez kłopotów usunąć". Podejście takie jest jednak o tyle problematyczne, że trudno jest antycypować wiedzę „przeciętnego użytkownika", bowiem użytkownik jakiegoś narzędzia informatycznego nabywa biegłości w jego użytkowaniu, nawet większej niż zawodowy informatyk, który się nim na co dzień nie posługuje. Niestety tego rodzaju pytania do biegłych informatyków spotyka się w praktyce całkiem często. W literaturze przedmiotu podnosi się również, że chodzi o ową istotność w sensie obiektywnym, a nie subiektywnym (zob. np.: A. Suchorzewska: *Ochrona*…, op. cit., s. 222 i 223), co zdaje się być o tyle słuszne, że np. czas unieruchomienia systemu po dokonaniu w nim jakichś niewłaściwych z technicznego punktu widzenia zmian, może być długi ze względu na brak interwencji serwisowej, choć usunięcie przyczyny takiego unieruchomienia może być dla serwisu stosunkowo proste, niemniej obiektywnie przez długi czas system był niedostępny (nie działał).

spodziewać się że przy ocenie owej istotności sąd będzie chciał zasięgnąć opinii biegłego informatyka. Należy pamiętać, że – w przeciwieństwie do medycyny sądowej, która wypracowała pewne intersubiektywne, umowne kryteria dotyczące zagadnień takich jak np. określenie czasu, na jaki naruszona została czynności narządu ciała[321] – informatyka nie wypracowała żadnych kryteriów w tym względzie, stąd biegły powinien unikać jakichkolwiek dywagacji. Sądu bowiem nie interesują (a przynajmniej nie powinny interesować) osobiste poglądy biegłego, ale stanowisko dyscypliny, którą biegły przed nim reprezentuje. Oczywiste wydaje się, że o istotnym stopniu zakłócenia pracy systemu lub sieci można mówić, jeśli doszło do długotrwałego przerwania ich ciągłości działania, natomiast ocena stopnia zakłócenia pracy systemu w innych przypadkach musi być rozpatrywana indywidualnie przez sąd.

4.6 Sabotaż komputerowy. Art. 269 KK

Przedmiotem ochrony czynu zabronionego określonego w art. 269 KK (zob. Tabela 1) zdaje się być[322] szczególny rodzaj danych informatycznych, mianowicie dane o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Warto na marginesie zwrócić uwagę, że nie musi to być organ czy instytucja państwa polskiego. Omawiany artykuł może znaleźć zastosowanie przy atakach na dane informatyczne o szczególnym znaczeniu dla organów innego niż Polska państwa. Drugą kwestią wartą odnotowania jest fakt, że nie każde

[321] Rozważania takie są istotne z uwagi na treść art. 157 KK, który rozróżnia naruszenie czynności narządu ciała lub rozstrój zdrowia na czas dłuższy i nie dłuższy niż 7 dni, podczas gdy zjawiska takie jak gojenie się ran przebiegają bez ostrej granicy czasowej. Konieczne było więc opracowanie kryteriów pozwalających na ujednolicenie opiniowania w tym względzie.

[322] Według B. Kunickiej-Michalskiej, zakres ochrony może sprawiać bardzo poważne trudności interpretacyjne (B. Kunicka-Michalska: *Komentarz*…, op. cit., s. 636). Według M. Siwickiego „należy przyznać rację tym autorom, którzy uznają, że przedmiotem ochrony tego przepisu nie jest bezpieczeństwo informacji, lecz obronność kraju, bezpieczeństwo w komunikacji oraz funkcjonowanie administracji publicznej" (M. Siwicki: *Cyberprzestępczość*, op. cit., s. 157). Por. też S. Koc, *Karnoprawna*…, op. cit., s. 122 i nast.

dane przetwarzane przez podmioty wymienione w dyspozycji artykułu muszą być danymi o szczególnym znaczeniu dla funkcjonowania tego organu, obronności kraju czy bezpieczeństwa w komunikacji[323].

Znamiona ustawowe czynów penalizowanych w pierwszym paragrafie tego artykułu pokrywają się częściowo ze znamionami przestępstwa stypizowanego w art. 268a KK, możliwe jest również, że art. 269 stanie się *lex specialis* dla szeregu innych artykułów KK[324].

4.7 Naruszanie integralności systemu. Art. 269a KK

Warto zwrócić uwagę, że dyspozycja tego artykułu (zob. Tabela 1) jest bardzo podobna do dyspozycji art. 268a § 1 KK. W komentarzach do omawianego przepisu, a także w projekcie zmian w Kodeksie karnym, rozważanym już w roku 2010 przez Ministerstwo Sprawiedliwości zauważono skądinąd słusznie, że rolą systemu informatycznego jest przetwarzanie, przekazywanie i gromadzenie danych informatycznych, z czego muszą wynikać niejasności interpretacyjne i trudności w stosowaniu tego przepisu w praktyce[325].

[323] Por. M. Siwicki: *Cyberprzestępczość*, op. cit., s. 158.

[324] Według B. Kunickiej-Michalskiej art. 269 KK jako *lex specialis* pochłonie art. 268 KK, a także 268a i 269a KK. Możliwe też jest, że art. 269 KK stanie się *lex specialis* dla artykułu 276 KK (przestępstwo niszczenia dokumentów). Zob. B. Kunicka-Michalska: *Komentarz*…, op. cit., s. 637; por. też np. S. Koc: *Karnoprawna*…, op. cit., s. 126 i nast.

[325] W projekcie zmian KK, o którym mowa (a który stał się, jak można przypuszczać, już nieaktualny) napisano: „Pierwszą usterką legislacyjną jest faktyczne powtórzenie dyspozycji art. 268a § 1 zdanie drugie KK przez art. 269a KK W art. 268a KK mowa jest o „istotnym zakłóceniu lub uniemożliwieniu automatycznego przetwarzania, gromadzenia lub przekazywanie danych informatycznych", w drugim zaś o „istotnym zakłóceniu pracy systemu komputerowego lub sieci teleinformatycznej". Pojęcia te można uznać za tożsame, gdyż cechą systemu lub sieci jest automatyczne przetwarzanie danych informatycznych (por. np. F. Radoniewicz: *Postanowienia decyzji ramowej Rady w sprawie ataków na systemy informatyczne a ujęcie cyberprzestępstw w Kodeksie karnym*, „Ius Novum" 2009/1/48 oraz W. Wróbel [w:] *Kodeks karny. Część szczególna. Komentarz*, T. II, pod red. A. Zolla, tezy do art. 269a, Kraków 2006). Jeżeli natomiast uznać, że pojęcia te nie są tożsame, to niewątpliwie zakłócenie przetwarzania danych mieści się w zakresie znaczeniowym zakłócenia pracy systemu komputerowego. Wskazane przy tym jest zachowanie pojęcia „systemu komputerowego" jako szerszego i odnoszącego się bezpośrednio do wspomnianej decyzji ramowej" (za: P. Waglowski: *Projekt zmian kodeksu karnego pod internetową choinkę*, http://prawo.vagla.pl/node/9299). Trudno się wprawdzie zgodzić, aby

Znamię czynu zabronionego w art. 268a KK jest o tyle szersze, że obejmuje również niszczenie, uszkadzanie, zmianę i utrudnienie dostępu do danych informatycznych, które nie zakłóca pracy systemu informatycznego (komputerowego)[326].

W przeciwieństwie do art. 268 i 268a KK, przestępstwa stypizowane w art. 269 KK są ścigane z urzędu. Rodzi to dodatkowe trudności w procesie subsumpcji, jeśli poszkodowany nie wystąpił z wnioskiem o ściganie.

Artykuły 269 KK oraz 269a KK mogą znajdować zastosowanie w przypadku ataków typu *Denial of Service*[327]. Kwestią problematyczną jest możliwość ich wykorzystania w przypadku niektórych ataków typu *Distributed Denial of Service*, szczególnie ataków polegających na przesyłaniu dużej liczby żądań standardowych usług (np. dużej liczby wyświetleń stron www). W przypadku artykułu 269a KK źródłem wątpliwości jest zapis „kto nie będąc do tego uprawnionym" (zazwyczaj osoby biorące świadomie udział w tego typu ataku DDoS są uprawnione do wyświetlenia zawartości strony), zaś w przypadku art. 269 KK – trudność z ustaleniem osoby zakłócającej działanie systemu i przypisaniem jej winy[328].

---

cechą sieci komputerowej było przetwarzanie danych, ale poza tą niezręcznością, należałoby przyznać rację komentatorowi.

[326] M. Siwicki pisze: „Przepis art. 269a KK zakresowo zbliżony jest z art. 268a KK. Przewiduje on jednak wyższe zagrożenie sankcją karną (...). Skłania to do wniosku, iż do realizacji znamion omawianego przepisu dochodzi wówczas gdy następuje kwalifikowane zakłócenie (tj. w istotnym stopniu) automatycznego przetwarzania, gromadzenia i przekazywania danych informatycznych, odnoszące się do całości funkcjonalnie wyodrębnionego systemu lub sieci". M. Siwicki: *Cyberprzestępczość*, op. cit., s. 159.

[327] Zob. ibid., s. 159: „Ataki typu *Denial of Service*, posługiwanie się tzw. złośliwym oprogramowaniem, bomby mailowe, mogą być inkryminowane w oparciu o art. 269 § 1 KK przewidujący karalność spowodowania zakłóceń lub uniemożliwienia automatycznego gromadzenia lub przekazywania informacji (sabotaż informatyczny), [w] sytuacji kiedy atak jest skierowany przeciwko domenom rządowym, zaś w przypadku ataków na serwery komercyjne na podstawie art. 269a KK". Przy czym warto pamiętać, że – jak wspomniano już wcześniej – nie każdy zasób informatyczny znajdujący się w domenie rządowej musi mieć szczególne znaczenie dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego itd.

[328] Tym bardziej, że w przypadku (prawdziwej, bądź nieprawdziwej) informacji o ataku na dany serwis duża liczba osób chcących sprawdzić, czy atak rzeczywiście miał miejsce generuje dodatkowy ruch poprzez próby wejścia na określone strony. Zob. np.: D. Lisiak Felicka, M. Szmit: *„Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland* [w:]

Artykuł 269a KK może też znaleźć zastosowanie przy penalizacji niektórych postaci *pharmingu* związanych z modyfikacją wpisów DNS[329].

4.8 Niewłaściwe użycie urządzeń. Art. 269b KK

Powołane w treści (zob. Tabela 1) przepisu artykuły dotyczą:

- ✓ zakłócania, uniemożliwiania lub wpływania w inny sposób na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych (art. 165 § 1 pkt 4 KK)[330];
- ✓ założenia lub posługiwania się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem w celu uzyskania informacji nieprzeznaczonej dla sprawcy (art. 267 § 3 KK);
- ✓ niszczenia, uszkadzania, usuwania, zmieniania i utrudniania dostępu do danych informatycznych oraz zakłócania w istotnym stopniu lub uniemożliwiania automatycznego przetwarzania, gromadzenia bądź przekazywania takich danych (art. 268a § 1 KK);
- ✓ niszczenia albo wymieniania informatycznego nośnika danych lub niszczenia albo uszkadzania urządzenia służącego do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych (art. 269 § 2 KK);
- ✓ transmisji, zniszczenia, usunięcia, uszkodzenia, utrudnienia dostępu i zmiany danych informatycznych (art. 269a KK).

Artykuł 269b KK trudno nazwać inaczej niż kuriozalnym, odwołując się bowiem do pojęcia urządzeń i programów przystosowanych do popełniania

W. Biały, J. Kaźmierczak, *Systems supporting production engineering*, pod red. W. Białego, J. Kaźmierczaka, s. 133–145, PKJS, Gliwice 2012.

[329] „W literaturze niejednokrotnie wskazywano już na problem krzyżowania się zakresów karalności art. 268a i art. 269a KK (…). Zdaje się więc, że czyn sprawcy należałoby zakwalifikować na podstawie obu zbiegających się przepisów, sąd natomiast winien wymierzyć karę na podstawie art. 269a KK, jako zawierającego wyższą sankcję karną. Sytuacja ta świadczy jednak o braku konsekwencji ustawodawcy" (A. Kiedrowicz-Wywiał: *Pharming i jego penalizacja*, „Prokuratura i Prawo" Nr 6/2011, s. 24–36).

[330] Warto na marginesie zauważyć, że art. 165 KK dotyczy sprowadzania niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach. Ustawodawca zamiast odwołać się do artykułu 268a i 269 KK odwołał się do artykułu z zupełnie innej części Kodeksu karnego (w którym zresztą znamiona czynów zabronionych zostały sformułowane bardzo szeroko).

przestępstw, literalnie rozumiany, zabrania w zasadzie posiadania jakiegokolwiek urządzenia komputerowego, któreś z wymienionych przestępstw da się bowiem na pewno popełnić posługując się dowolnym urządzeniem i większością programów[331], włączając w to systemy operacyjne, które posiadają przecież narzędzia przystosowane do transmisji czy zmiany danych informatycznych. Z powodu swojej ułomnej konstrukcji art. 269b KK pozostaje przepisem *de facto* martwym[332]. W zasadzie jedynym możliwym zastosowaniem tego artykułu jest ewentualne ściganie twórców złośliwego oprogramowania (np. wirusów komputerowych), choć wydaje się, że – wobec tak fatalnej konstrukcji przepisu – znacznie lepiej jest stosować jakikolwiek przepis dotyczący zastosowania takiego narzędzia (a więc przede wszystkim naruszenie integralności danych czy oszustwo). Wobec powyższego trudno w zasadzie omawiać rolę biegłego informatyka w odniesieniu do tego przepisu. Można wspomnieć tylko o ustawowym znamieniu „pozyskiwania" znajdującym się w dyspozycji tego artykułu. Jak się wydaje można tu przeprowadzić rozumowanie podobne jak w przypadku znamienia „sprowadzania" użytego w art. 202 § 4a KK (zob. rozdział 5.1), przy czym warto wspomnieć, że w literaturze przedmiotu podejmowane były próby rozszerzającej interpretacji tego znamienia[333], które wydają się być zdecydowanie zbyt daleko idące.

---

[331] Są one bowiem przystosowane do wykonywania takich czynności (zarówno jeśli przez „przystosowany" będziemy rozumieć „dopasowany", „możliwy do wykorzystania", jak i jeśli słowo to zinterpretujemy jako „celowo przysposobiony").

[332] Por. Tabela 4.

[333] K. Gienias pisze: „Omawiany przepis wśród znamion czynu zabronionego pomija posiadanie »narzędzi hackerskich«. Cóż z tego, skoro przepis penalizuje ich »pozyskiwanie«. Mamy więc do czynienia *de facto* z możliwością pociągnięcia do odpowiedzialności karnej użytkownika, który na swoim twardym dysku przechowuje narzędzia służące popełnianiu cyberprzestępstw. Jest to przecież naturalna konsekwencja ich pozyskania, przy czym z perspektywy art. 269b KK znaczenia nie ma, w jaki sposób sprawca dotarł do tego typu narzędzi. Jednocześnie dla skutecznego zastosowania przepisu, wystarczy ujawnienie choćby jednego »narzędzia hackerskiego«" (K. Gienias: *Eliminacja „Rajów Hackerskich" czy ograniczenie metod badania systemów informatycznych* [w:] J. Kosiński: *Przestępczość teleinformatyczna: IX seminarium naukowe: materiały seminaryjne*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2006, s. 31–38). Jest to oczywiście rozumowanie niepoprawne (podobnie jak w przypadku znamienia sprowadzania z art. 202 § 3 i § 4a KK): w posiadanie czy to treści, czy programów można wejść w najróżniejszy sposób, choćby przez zainfekowanie systemu wirusem

4.9 Fałszerstwo komputerowe

Podstawowa postać przestępstwa fałszerstwa dokumentów stypizowana jest w art. 270 § 1 KK

Art. 270.

§ 1. Kto, w celu użycia za autentyczny, podrabia lub przerabia dokument lub takiego dokumentu jako autentycznego używa, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto wypełnia blankiet, zaopatrzony cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo takiego dokumentu używa.

§ 2a. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 3. Kto czyni przygotowania do przestępstwa określonego w § 1, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

W tym samym XXXIV rozdziale KK stypizowano szereg innych przestępstw przeciwko wiarygodności dokumentów. Również w innych przepisach spenalizowno szczególne rodzaje fałszerstwa (np. fałszerstwo znaków pieniężnych – art. 310), nie wyodrębniono natomiast w krajowych przepisach kwalifikowanej formy przestępstwa fałszerstwa danych informatycznych. W konsekwencji fałszerstwo danych informatycznych może wypełniać znamiona poszczególnych rodzajów fałszerstwa, o których mowa powyżej. Biorąc pod uwagę, że fałszerstwo dokumentu elektronicznego może się wiązać z jego nieuprawnioną modyfikacją (a więc z naruszeniem

lub robakiem komputerowym. Niewątpliwie z jednej strony jest to oprogramowanie przystosowane (a nawet celowo zaprojektowane) do niszczenia, uszkadzania, usuwania, zmieniania lub utrudniania dostępu do danych informatycznych albo zakłócania w istotnym stopniu lub uniemożliwiania automatycznego przetwarzania, gromadzenia lub przekazywania takich danych, z drugiej zaś strony jego posiadacz wchodzi w posiadanie tego oprogramowania bez swojej wiedzy, a nawet wbrew własnej woli, nie można mu więc przypisać winy. Dysk zawierający takie oprogramowanie można kupić (nie wiedząc o jego zawartości), można być nim obdarowanym, można go odziedziczyć itd. Nie można także zapominać o fakcie, że komputer może być używany przez różne osoby, a nawet być ich współwłasnością i – szczególnie w przypadku oprogramowania darmowego, pobranego z publicznych serwisów internetowych – trudno będzie ustalić osobę pozyskującą oprogramowanie.

integralności) może w poszczególnych przypadkach dojść również do popełnienia przestępstw stypizowanych w art. 268, 268a i 269 KK.

4.10 Oszustwo i szkodnictwo komputerowe. Art. 287 KK

Art. 287

§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Tak zwane oszustwo komputerowe jest stypizowane w art. 287 KK w rozdziale przestępstw przeciwko mieniu i zagrożone karą pozbawienia wolności od 3 miesięcy do lat 5, a w przypadkach mniejszej wagi – karą ograniczenia wolności albo pozbawienia wolności do roku. Mimo powszechnie przyjętej nazwy, trudno uznać oszustwo komputerowe za uprzywilejowaną formę oszustwa, co więcej, sytuację, w której sprawca wpływa na przetwarzanie danych informatycznych, po to, aby inną osobę wprowadzić w błąd i doprowadzić do niekorzystnego rozporządzenia mieniem kwalifikuje się jako przestępstwo oszustwa z art. 286 § 1 KK, a nie jako przestępstwo oszustwa komputerowego[334]. Istotną cechą przestępstwa z art. 287 KK jest wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych, bądź zmiana, usunięcie albo wprowadzanie nowego zapisu danych informatycznych; nie zachodzi więc tu sytuacja oddziaływania

[334] Zob. M. Siwicki: *Cyberprzestępczość*, op. cit., s. 257; A. Adamski: *Prawo...*, op. cit., s. 115–116.

Art. 286.

§ 1. Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

na osobę, a na techniczne procesy obróbki danych w systemie informatycznym, bądź na same dane. W konsekwencji art. 287 może stanowić *lex specialis* dla art. 269a, 268, 268a § 1 KK[335], a nawet art. 267 § 1 KK[336].

Przestępstwo stypizowane w art. 287 KK jest przestępstwem celowym, przy czym z uwagi na dwojaki cel można rozróżnić działanie w celu osiągnięcia korzyści majątkowej oraz działanie w celu wyrządzenia innej osobie szkody[337].

---

[335] Zob. M. Siwicki: *Cyberprzestępczość*, op. cit., s. 256.

[336] Zob. A. Adamski: *Prawo...*, op. cit., s. 117.

[337] Pojęcia szkody i korzyści majątkowej są interpretowane bardzo szeroko. Na przykład omawiany przepis znajduje zastosowanie w przypadku kradzieży wirtualnych artefaktów w grach MMORPG (ang. *Massively Multiplayer Online Role Playing Game*). Zob. P. Waglowski: *Jak wynika z doniesień policji: również bandyci grają w Tibia*, http://prawo.vagla.pl/node/9092; P. Waglowski: *Wirtualny miecz*, http://prawo.vagla.pl/node/188; P. Waglowski: *Ukradli wirtualną broń*, http://prawo.vagla.pl/node/3212; P. Waglowski: *Kradzież a usuwanie danych informatycznych – do Polski przybyły sprawy o "kradzież artefaktów" w grach MMORPG*, http://prawo.vagla.pl/node/9235; P. Waglowski: *Umowa o przeniesienie prawa do korzystania z awatarów i artefaktów*, http://prawo.vagla.pl/node/6065; *Kto zabrał broń za 900 zł postaci z gry internetowej*, http://olsztyn.gazeta.pl/olsztyn/1,35189,8181779,Kto_zabral_bron_za_900_zl_postaci_z_gry_internetowej.html; *Realni złodzieje w wirtualnych grach,* http://policyjni.gazeta.pl/Policyjni/1,103617,8779549,Realni_zlodzieje_w_wirtualnych_grach.html; *Złodziej wirtualnych butów otrzymał prawomocny wyrok,* http://polygamia.pl/Polygamia/1,107162,8511906,Zlodziej_wirtualnych_butow_otrzymal_prawomocny_wyrok.html; *17-latkowi grozi poprawczak za wirtualną kradzież*, http://www.dzienniklodzki.pl/artykul/425623,17latkowi-grozi-poprawczak-za-wirtualna-kradziez,id,t.html; J. Kulesza, J. Kulesza: *Gra „Second Life" – wirtualny świat, realne przestępstwa?*, „Prokuratura i Prawo" Nr 3/2009, s. 23–40; Co stosunkowo dziwne, ciągle jeszcze spotykane są próby prawnokarnej kwalifikacji takich czynów jak zwykłej kradzieży zob. np.: *Ukradł zbroję rycerzowi... z gry sieciowej*, http://krakow.gazeta.pl/krakow/1,44425,10655840,Ukradl_zbroje_rycerzowi____z_gry_sieciowej.html; *Policja zajmuje się kradzieżą w wirtualnym świecie*, http://polska.newsweek.pl/policja-zajmuje-sie-kradzieza-w-wirtualnym-swiecie,62499,1,1.html; *15-latka ukradła ekwipunek wirtualnemu wojownikowi*, http://www.policja.pl/pol/aktualnosci/84554,dok.html; podczas gdy oczywiście wirtualne artefakty nie są rzeczami. Można ewentualnie rozpatrywać je jako mienie (por. np. K. Grzybczyk, A. Auleytner, K. Kulesza: *Prawo w wirtualnych światach*, pod red. K. Grzybczyka, Difin, Warszawa 2013, s. 302; zob. też J.A. Pakuła: *Konta na serwerach gier internetowych w obrocie prawnym – zagadnienia węzłowe*, Warszawa 2009, praca magisterska, maszynopis, http://prawo.vagla.pl/files/mgr_j_a_pakula.pdf) takim bowiem mogą być prawa majątkowe. Powołani autorzy wywodzą, że gracz w grę MMORPG uzyskuje takowe w drodze licencji na używanie gry, stąd też kradzież artefaktu jest pozbawieniem go tych praw, co stanowi o możliwości klasyfikacji takiego czynu jako wypełniającego znamiona przestępstwa z art. 115 ust. 3 PrAut. Jak się wydaje tego ro-

Ten drugi przypadek nazywa się czasami przestępstwem szkodnictwa komputerowego[338].

Przestępstwo oszustwa (i szkodnictwa) komputerowego ma bardzo szeroko określone znamiona czynów zabronionych (przy czym – dla odróżnienia od ustawowych znamion czynów zabronionych stypizowanych w art. 268, 268a i 269 KK) ustawodawca zdecydował się na wymienienie wśród tych znamion wprowadzania nowych zapisów danych informatycznych[339]. Z punktu widzenia biegłego warto zwrócić uwagę na jeden szczegół związany z nowelizacją Kodeksu karnego z 2004 r. Przed ową nowelizacją omawiany artykuł brzmiał:

§ 1. Kto w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

---

dzaju rozumowanie jest o tyle ryzykowne, że po pierwsze przepisy tego ustępu są krytykowane za swoją nieokreśloność (11 kwietnia 2013 r. Rzecznik Praw Obywatelskich skierował do Trybunału Konstytucyjnego wniosek o zbadanie tego ustępu z art. 42 Konstytucji RP, obecnie sprawa znajduje się w Trybunale – K 15/13, http://trybunal.gov.pl/s/k-1513/), po wtóre należałoby bardzo dokładnie rozpatrywać, jakie prawa przyznaje licencja użytkownikowi gry (i jak zapisy licencji mają się do przepisów prawa polskiego, co bardzo często sprawia problemy, bowiem spora część gier jest tworzona w innych systemach prawnych, a ich licencje zawierają trudne do zinterpretowania w warunkach polskiego systemu prawnego konstrukcje), po trzecie wreszcie trudno wątpić, że zabór artefaktu w grze komputerowej nie wyczerpuje znamion dyspozycji art. 287 KK. Oczywiście każdorazowo przy kwalifikacji prawnej czynu należy rozpatrzeć *modus operandi* sprawcy, który może wyczerpywać ustawowe znamiona innych przestępstw. W powołanej w przypisie pracy K. Grzybczyka, A. Auleytnera, K. Kuleszy, przytoczone są przykłady, w których wejście w posiadanie wirtualnych artefaktów, bądź awatarów było skutkiem wymuszenia na ich posiadaczu ujawnienia haseł dostępowych na drodze gróźb czy pobicia.

[338] Zob. np.: S. Łagodziński: *Przestępstwa przeciwko mieniu w kodeksie karnym (wybrane zagadnienia)*, „Prokuratura i Prawo" Nr 2/1999.

[339] Tego rodzaju niechlujstwo ustawodawcy może mieć poważne konsekwencje na sali sądowej, można bowiem podnosić argument, że jeśli ten sam racjonalny ustawodawca (a założenie o racjonalności ustawodawcy należy do podstawowych założeń wykładni prawa) wśród ustawowych znamion jednego czynu zabronionego wymienia owo „wprowadzanie nowego zapisu", zaś wśród znamion innego czynu już nie, to zapewne jego wolą było pozostawienie takiego działania (naruszania integralności poprzez wprowadzanie nowych zapisów) poza zakresem karalności.

§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Wprowadzona zmiana („danych informatycznych" zamiast „informacji" oraz – co istotniejsze – zamiast „zapis na komputerowym nośniku informacji") spowodowała zawężenie znamion czynu zabronionego, w ten sposób, że nie jest już penalizowane (przynajmniej w tym przepisie można bowiem zastanawiać się nad implikacjami takiego działania w świetle przepisów prawa autorskiego) zmienianie, usuwanie ani wprowadzanie nowych zapisów w programie komputerowym (o ile oczywiście wtórnie owe zmiany nie spowodują takiego działania programu, które odpowiadałoby realizacji ustawowych znamion czynu zabronionego, tj. np., że tak zmodyfikowany program nie usunie jakichś danych informatycznych).

5 Opiniowanie w innych szczególnych rodzajach spraw

Wśród innych rodzajów spraw, z jakimi ma do czynienia biegły informatyk, warto zwrócić szczególną uwagę na postępowania dotyczące przestępstw kontentowych, w których rolą informatyka jest ujawnienie treści dokumentów elektronicznych, jak również okoliczności ich utworzenia i przetwarzania na postępowania dotyczące programów komputerowych oraz – z powodu szeregu ograniczeń proceduralnych – na postępowania cywilne.

5.1 Opiniowanie w sprawach przestępstw kontentowych na przykładzie art. 202 KK[341]

Rolą biegłego informatyka przy okazji przestępstw związanych z treścią informacji jest przede wszystkim ujawnienie tejże treści[342] (najczęściej danych zapisanych na cyfrowym nośniku informacji, rzadziej – przesyłanych przez sieć komputerową w czasie jej obserwacji „na żywo") oraz – na podstawie metainformacji z zabezpieczonego sprzętu (logów systemowych,

[341] Wykorzystano fragmenty artykułu M. Szmit: *Kilka uwag o zadaniach biegłego informatyka w postępowaniu przygotowawczym w sprawach z art. 202 KK*, „Diariusz Prawniczy" Nr 16–17/2012, s. 97–108.

[342] Zgodnie z tym, co napisano powyżej, w sprawach karnych KPK obliguje organ procesowy do zasięgnięcia opinii biegłych, jeżeli stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych. Można domniemywać, że – przynajmniej na obecnym etapie rozwoju techniki – badanie zawartości urządzeń informatycznych nie zalicza się do kanonu wiedzy ogólnej. Przeciwnie – stosunkowo liczne przypadki kontaminacji dowodów elektronicznych wskazują, że nawet osoby z kierunkowym wykształceniem informatycznym nie zawsze posiadają odpowiednią do tego celu wiedzę i praktykę, tak więc obecność biegłego informatyka w sprawach przestępstw „kontentowych" wymagających ujawnienia treści dowodów elektronicznych wydaje się być obligatoryjna, a na pewno jest wskazana.

metadanych systemu operacyjnego czy poszczególnych rodzajów dokumentów[343]) – określenie okoliczności, w jakich treści te znalazły się na komputerze oraz czynności, jakim były poddane, w szczególności jeśli mogły to być czynności penalizowane w dyspozycji artykułu, o którym mowa (np. rozpowszechnianie pliku w Internecie).

Konstrukcja art. 202 KK jest interesująca również z tego punktu widzenia, że zawiera całą gamę znamion czasownikowych, które oznaczają czynności, jakie – zdaniem ustawodawcy – można wykonać z treścią informacji[344]. Artykuł 202 KK penalizuje posiadanie, produkowanie, sprowadzenie, prezentowanie, udostępnianie, utrwalanie, rozpowszechnianie, przechowywanie i uzyskiwanie dostępu różnych rodzajów treści pornograficznych, a także uczestnictwo w prezentacji treści pornograficznych celu zaspokojenia seksualnego. Obecna redakcja tego artykułu jest wynikiem szeregu zmian legislacyjnych, które ustawodawca w kolejnych latach wprowadzał[345], usiłując m.in. nadążyć za rozwojem współczesnych narzędzi informatycznych oraz próbując dostosować polskie prawo do dyrektyw i konwencji międzynarodowych. Proces ten doprowadził do powstania zapisów mających charakter wybitnie kazuistyczny, niekiedy pozornie skrajnie restrykcyjnych, które jednak trudno jest stosować w praktyce.

Poniżej omówiono te spośród wymienionych w powołanym artykule czynności, których sposób realizacji może budzić wątpliwości z punktu widzenia biegłego informatyka, a o które może być zapytany przez organ procesowy.

Ustawowe znamię rozpowszechniania definiuje się zazwyczaj jako „uczynienie powszechnie dostępnym", „stworzenie możliwości publiczne-

[343] W szczególności np. dla zdjęć zapisanych w formacie JPG przechowywane mogą być obszerne dane np. o typie aparatu fotograficznego, dacie i miejscu wykonania zdjęcia itd.

[344] Wśród czasowników jakich użył ustawodawca brak właściwie tylko „uzyskiwania", o którym była mowa przy okazji art. 269b KK (rozdział 4.8).

[345] Oprócz ustawy z 4 kwietnia 2014 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. 2014 poz. 538), mowa o następujących ustawach: ustawa o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń z 18 marca 2004 r. (Dz.U. Nr 69, poz. 626), ustawa o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego i ustawy – Kodeks karny wykonawczy z 27 lipca 2005 r. (Dz.U. Nr 163, poz. 1363) oraz ustawa o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw z 24 października 2008 r. (Dz.U. Nr 214, poz. 1344).

go dostępu”[346], „uczynienie dostępnym dla nieokreślonej liczby odbiorców”[347], ale można spotkać się też z restrykcyjnym stanowiskiem, że „znamię rozpowszechniania będzie zrealizowane również w przypadku czynności jednorazowej polegającej na dostarczeniu określonej treści pornograficznej konkretnej osobie, jednakże dokonane ze świadomością, iż treści te zostaną następnie przekazane przez nią innym osobom”[348]. W kontekście interesującym z punktu widzenia rozważanych zagadnień, istotne jest najczęściej, czy dane znajdujące się w badanym komputerze były – przy wykorzystaniu technik informatycznych – udostępniane osobom innym niż użytkownik tego komputera[349].

Udostępnianie bądź przekazywanie danych pomiędzy użytkownikami różnych komputerów może mieć miejsce na wiele sposobów. Dane można skopiować pomiędzy komputerami, począwszy od wykorzystania nośników zewnętrznych (pamięć USB, płyty CD/DVD/BD, dyskietki), poprzez

[346] Zob. np.: R. Krajewski: *Przestępstwo utrwalania i rozpowszechniania wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej*, „Prokuratura i Prawo” Nr 5/2012 s. 20–40.

[347] Taka wykładnia funkcjonuje przynajmniej w zakresie prawa autorskiego, w kontekście rozpowszechniania utworów. Por.: J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski: *Prawo autorskie i prawa pokrewne. Komentarz*, Wolters Kluwer, Warszawa 2011, s. 747. Również w pracy A. Grześkowiak, K. Wiak: *Kodeks karny. Komentarz*, pod red. A. Grześkowiak i K. Wiaka, C.H. Beck, Warszawa 2012, autorzy piszą: „Rozpowszechnianie treści pornograficznych to m.in. kolportaż, publikacja, użyczenie, kopiowanie i innego rodzaju udostępnianie takich treści szerszemu i bliżej nieokreślonemu kręgowi osób. Nie stanowi natomiast rozpowszechniania działanie polegające na udostępnieniu treści pornograficznych niewielkiemu i ściśle określonemu kręgowi osób (wyrok SN z 16.2.1987 r., WR 28/87, OSNKW Nr 910/1987, poz. 85)”.

[348] P. Siemkowicz: *Przestępstwa o charakterze pedofilskim i przeciwko wolności seksualnej popełniane poprzez Internet, w ujęciu polskiego kodeksu karnego*, „e-Czasopismo Prawa Karnego i Nauk Penalnych” Nr 7/2011, http://www.czpk.pl/artykuly/7-2011-Siemkowicz_P._Przestepstwa_o_charakterze_pedofilskim_i_przeciwko_wolnosci_seksualnej_popelniane_poprzez_Internet_w_ujeciu_polskiego_kodeksu_karnego.pdf.

[349] Warto na marginesie zauważyć, że trudności może sprawiać samo określenie, kto dopuścił się czynu zabronionego, jeśli użytkowników komputera było wielu: w takim przypadku pomocne mogą być informacje o kontach użytkowników skonfigurowanych na badanym urządzeniu czy metadane dotyczące czasu operacji na konkretnych plikach (utworzenia, pobrania, udostępnienia, modyfikacji itd.).

przesyłanie przy wykorzystaniu mechanizmów poczty elektronicznej[350], aż do wykorzystania różnych rodzajów serwisów i aplikacji sieciowych. Stosunkowo najbardziej rozpowszechnionym sposobem (szczególnie wśród mało zaawansowanych użytkowników) są sieci *peer-to-peer* (P2P)[351]. Obsługa protokołów P2P wbudowana jest w niektóre przeglądarki internetowe (bądź też wtyczki do nich), stąd też do rozpowszechniania plików w sieci P2P nie jest konieczne posiadanie dedykowanych programów[352].

Warto pamiętać, że z punktu widzenia przeciętnego użytkownika, pobranie pliku z serwera www i z sieci P2P wygląda podobnie, dlatego też spora część użytkowników sieci P2P nie zdaje sobie sprawy, że „ściągając" jakiś plik jednocześnie udostępnia go innym, co wyczerpuje ustawowe znamię rozpowszechniania (dotyczy to zresztą również przestępstw z art. 116 PrAut). Nieznajomość architektury i zasady działania sieci P2P jest zresztą jedną z linii obrony osób rozpowszechniających treści za ich pomocą. Rzecz jasna, biegły informatyk nie jest w stanie wspomóc tu organu procesowego w dotarciu do prawdy, nie posiada bowiem wglądu w wiedzę użytkownika komputera. Stąd też, zdarzające się niestety dość często w postanowieniach o zasięgnięciu opinii biegłego, pytania: „czy użytkownik komputera rozpowszechniał pliki w sposób świadomy", muszą pozostać bez odpowiedzi.

Wiąże się z tym również kwestia sformułowania „kto, w celu" z art. 202 § 3 KK, które to sformułowanie implikuje zawężenie strony podmiotowej przestępstwa do zamiaru kierunkowego i eliminuje zamiar ewentualny.

---

[350] Na szczególne uwzględnienie zasługuje wykorzystanie darmowych skrzynek pocztowych do rozpowszechniania plików (tzw. *peer-to-mail* P2M) oraz wykorzystanie do tego celu serwerów news (NNTP – *Network News Transfer Protocol*).

[351] Samo pojęcie P2P pierwotnie odnosiło się do architektury przetwarzania rozproszonego. Zasadniczo istnieją dwa rodzaje architektur: klient/serwer (ang. *Client/Server, C/S*) oraz *Peer-to-Peer* (ang. *peer* – równorzędny). W architekturze *Peer-to-Peer* maszyna korzystająca z usługi jest jednocześnie jej dostawcą. Architektura ta jest wykorzystywana m.in. do pobierania/rozpowszechniania plików, głównie z tego powodu, że model P2P pozwala rozłożyć obciążenie na wiele maszyn – komputery pobierające plik jednocześnie go udostępniają, a kolejne żądania pobrania pliku kierowane są przez odpowiednie mechanizmy sieciowe do różnych dostawców, tak aby uniknąć powstawania „wąskich gardeł" transmisji i nadmiernego obciążenia komputera udostępniającego dane, co zdarza się w przypadku pojedynczych serwerów w architekturze C/S.

[352] Nie do końca poprawnie zwanych klientami, takich jak np. MicroTorrent czy Azureus.

Trudność polega tu na tym, że nawet rozpowszechnianie określonego rodzaju materiałów nie jest wystarczające (wobec nieznajomości zasad działania narzędzia, z którego osoba pobierająca/rozpowszechniająca treści korzystała) do niebudzącego wątpliwości udowodnienia, że rzeczywiście miała ona zamiar rozpowszechniania. Z drugiej strony możliwe jest również korzystnie z sieci P2P przy użyciu oprogramowania skonfigurowanego tak, aby nie pozwalało ono na rozpowszechnianie pobranych plików[353]. Z tego powodu samo znalezienie adresu IP komputera na liście adresów, które pobierały dany plik w sieci P2P nie jest wystarczające do stwierdzenia, że plik ten był z komputera o tym adresie również udostępniany.

Podobna linia obrony dotyczy często posiadania[354] poszczególnych rodzajów materiałów pornograficznych, penalizowanego w paragrafach 3, 4, 4a oraz 4b omawianego artykułu. Pojawia się tu zresztą kilka dodatkowych problemów:

- ✓ po pierwsze, użytkownik systemu komputerowego mógł wejść w posiadanie „treści zabronionych" w sposób przypadkowy. W Internecie, a w szczególności w sieciach P2P, można znaleźć pliki, które pod stosunkowo „niewinnymi" nazwami zawierają materiały pornograficzne, w tym pornografię dziecięcą. Rzeczywiście trudno nie dać wiary takiemu tłumaczeniu, jeśli na badanym komputerze znaleziono pojedyncze zdjęcie czy film, znajdujące się w pliku o nazwie sugerującej zupełnie inną zawartość. Drugą skrajnością są „kolekcjonerzy", którzy różne rodzaje materiałów pornograficznych przechowują na starannie opisanych i skatalo-

[353] Jakkolwiek twórcy sieci P2P usiłują bronić się przed taką możliwością (z technicznego punktu widzenia istnienie tego rodzaju klientów sieci powoduje wzrost jej obciążenia i utratę korzyści, jakie architektura P2P daje w stosunku do architektury C/S), to istnieje oprogramowanie umożliwiające osiągnięcie takiego efektu. W szczególności, dla sieci BitTorrent jest to klient o nazwie Bitthief, http://bitthief.ethz.ch. Dokładne informacje o zasadzie jego działania zawiera artykuł T. Locher, P. Moor, S. Schmid, R. Wattenhofer: *Free Riding in BitTorrent is Cheap*, http://www.disco.ethz.ch/publications/hotnets06.pdf.

[354] Zob. A. Piaczyńska: *Posiadanie jako znamię czynu zabronionego*, „Prokuratura i Prawo" Nr 7–8/2010, s. 54–70.

gowanych płytach CD/DVD. W takiej sytuacji pytanie o celowy charakter takiej działalności wydaje się mieć oczywistą odpowiedź[355];

- ✓ po wtóre, komputer użytkownika mógł zostać zainfekowany złośliwym oprogramowaniem, za pośrednictwem którego inna osoba przejęła nad nim kontrolę w sposób niezauważony przez jego „legalnego" użytkownika i wykorzystała do popełnienia czynów przestępnych. Biorąc powyższe pod uwagę, jest dobrą praktyką biegłych informatyków (pozostającą niestety bardzo często w sferze „dobrej teorii") uwzględnianie zawsze i w każdej opinii informacji o ewentualnym znalezionym w systemie komputerowym złośliwym oprogramowaniu. Jest to informacja na tyle istotna dla ustalenia prawdy, że powinna być uwzględniona w każdym wypadku, nawet jeśli zakres opinii określony w postanowieniu o jej zasięgnięciu nie zawiera *explicite* pytania o złośliwe oprogramowanie[356];
- ✓ po trzecie, podobna sytuacja może mieć miejsce w przypadku podszycia się (ang. *spoofing)* pod użytkownika w sieci, co szczególnie dotyczyć może osób, które korzystają z niezabezpieczonej lub źle zabezpieczonej sieci bezprzewodowej, bądź w przypadku kradzieży tożsamości;
- ✓ po czwarte wreszcie – może również mieć miejsce sytuacja, w której posiadacz nośnika wszedł nieświadomie w posiadanie treści na nim zawartych (np. przez nabycie używanego nośnika danych).

Z zagadnieniem posiadania wiąże się również kwestia określenia ustawowych znamion czynu zabronionego, w odniesieniu do treści przetwarza-

[355] Niemniej nie można takiego pytania zadawać biegłemu informatykowi – ocena stanu świadomości podejrzanego nie wchodzi bowiem w zakres wiadomości specjalnych z informatyki.

[356] Można podać przynajmniej dwa argumenty przemawiające za takim podejściem do tego zagadnienia: po pierwsze, z uwagi na zasadę prawdy materialnej – brak wiedzy organu procesowego o okoliczności, o której mowa, może skutecznie uniemożliwić dotarcie do niej; po drugie w literaturze poświęconej opiniowaniu (zob. np.: J. Wójcikiewicz: *Ekspertyza…*, op. cit., s. 27 i nast.) podkreśla się, że biegły ma nie tylko prawo, ale i obowiązek poinformować organ procesowy o podejrzeniu popełnienia przestępstwa, o którym dowiedział się na skutek realizacji czynności badawczych związanych z opiniowaniem, a niewątpliwie zainstalowanie takiego oprogramowania i zdalne uzyskanie w ten sposób dostępu do systemu informatycznego wyczerpuje znamiona przestępstwa z art. 267 § 2 KK.

nych w postaci elektronicznej. W najbardziej restrykcyjnym podejściu[357]: „Posiadanie jest czynem intencjonalnym, zaś przechowywanie nie. W przypadku komputerów – automatyczne zapisanie się zdjęcia w pamięci podręcznej oznacza przechowywanie, zaś świadome zapisanie pliku na dysk – posiadanie". Taką interpretację należy uznać za błędną[358]. Pomijając już, że „automatyczne" zapisanie treści, np. przeglądanych stron www w pamięci podręcznej można ewentualnie, w niektórych rodzajach przeglądarek i systemów operacyjnych wyłączyć (co jednak wymaga od użytkownika komputera pewnej wiedzy i umiejętności), to i tak, aby móc zapoznać się z treścią dowolnego dokumentu, wykorzystując w tym celu komputer trzeba dokument ten w jakiś sposób przekazać do odpowiedniego urządzenia wyjścia (monitora, rzutnika, drukarki, czy w przypadku utworów dźwiękowych – na głośniki podłączone do wyjścia audio), co implikuje konieczność umieszczenia takiego dokumentu w pamięci operacyjnej tego komputera (ang. *Random Access Memory*, RAM). W ten sposób przesłanki czynu zabronionego byłyby spełnione np. przy odebraniu listu e-mail – jak również zwykłego listu papierowego – zawierającego „treści zabronione" (już przed zapoznaniem się adresata z jego treścią), czy przy przypadkowym wejściu na stronę www zawierającą takie treści (choćby osoba, która na tę stronę weszła, natychmiast zamknęła przeglądarkę czy opuściła stronę). Rzecz jasna, osobie takiej nie można byłoby przypisać winy za popełnienie tego rodzaju czynu.

Ustawowe znamię „przechowywania" znacznie lepiej wyjaśnia definicja, w myśl której: „za przechowywanie uznaje się taki stan, w którym zabezpiecza się określone treści w taki sposób, aby istniała możliwość zapoznania się z nimi w późniejszym okresie, a także posiadanie ich w ukryciu"[359]. Stąd też

[357] Zob. J. Śpiewak: *Wykorzystanie seksualne dziecka w kodeksie karnym od czerwca 2010 r.*, http://placzdziecka.blox.pl/html/1310721,262146,21.html?536592.

[358] Por. np.: A. Lach: *Pojęcie posiadania pornografii dziecięcej w art. 202 § 4a kodeksu karnego w odniesieniu do danych informatycznych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" Rok LXXII – Zeszyt 1 – 2010, s. 69-80; J. Warylewski: *System Prawa Karnego. T. 10. Przestępstwa przeciwko dobrom indywidualnym*, pod red. J. Warylewskiego, Warszawa 2012, Legalis.

[359] A. Marek: *Kodeks karny. Komentarz*, Wolters Kluwer, Warszawa 2007, s. 396 za: M. Wrześniewski: *Krytycznie o przestępstwach pornograficznych*, „Prokuratura i Prawo" Nr 11/2011, s. 98–111.

właściwe byłoby rozróżnienie, czy ewentualne „treści zabronione" znajdujące się na badanym nośniku danych znalazły się tam na skutek „automatycznych" działań systemu komputerowego (dotyczyć to będzie np. tworzonych lokalnie przez przeglądarkę internetową kopii przeglądanych stron www), czy też były zapisane przez użytkownika komputera. Ewentualna konkluzja opiniującego: „pliki, o których mowa znajdowały się wyłącznie w miejscach, w których przeglądarka przechowuje kopie buforowe", jest przesłanką przemawiającą za tym, że użytkownik komputera nie stawiał sobie za cel zapoznawania się nimi w późniejszym okresie[360].

Znalezienie się plików w pamięci buforowej przeglądarki (w praktyce również znalezienie przez biegłego na dysku plików uprzednio skasowanych, co do których nie można mieć pewności, że nie były umieszczone tylko w pamięci buforowej przeglądarki[361]) nie wyczerpuje również znamienia ich sprowadzania[362]. Warto natomiast pamiętać, że samo umieszczenie plików

[360] Oczywiście może się zdarzyć, że użytkownik przeglądarki celowo wykorzystywać będzie takie miejsce (ten sam folder, katalog) do przechowywania „treści zabronionych", choć jest to raczej mało prawdopodobne, ewentualnie jakichś informacji może dostarczyć analiza dat ostatniego dostępu do plików, choć wnioskowanie z tego rodzaju metadanych prowadzi zazwyczaj do konkluzji o niewielkiej stanowczości.

[361] W przypadku niektórych systemów operacyjnych i niektórych metod usuwania plików nie można ustalić w jakim katalogu (folderze) znajdowały się one pierwotnie.

[362] Szczegółowo wyjaśnia to fragment uzasadnienia wyroku Sądu Apelacyjnego we Wrocławiu z 27 września 2012 r. (II AKa 171/12):

„Sprowadzanie to tyle co spowodowanie przybycia, znalezienia się czegoś w jakimś miejscu, przyczynienie (*Słownik języka polskiego* pod red. M. Szymczaka, Warszawa 1993, t. III s. 306). Chodzi więc zarówno o przemieszczenie się czegoś, jak i zachowanie nakierowanie by to przybycie, pojawienie się spowodować. M. Rodzynkiewicz uważa, że czasownik ten użyty w art. 202 § 4a KK oznacza tak obrót zagraniczny, jak i krajowy, a także »sprowadzanie zakazanych treści z sieci internetowej niezależnie od tego gdzie znajduje się serwer, na którym umieszczono te treści« (*Kodeks karny. Część szczególna, T. II. Komentarz*, pod red. A. Zolla teza 29 do art. 202 KK). Podobnie A. Marek (A. Marek: *Kodeks karny. Komentarz*, LEX 2010. Teza 9 do art. 202 KK) wskazujący, że chodzi o pozyskiwanie takich treści. Widoczne jest powiązanie tego znamienia z pozostałymi wymienionymi w art. 202 § 4 a KK jako wstępnego etapu mogącego prowadzić do posiadania lub przechowywania nośników treści pornograficznych. Przedstawiony sposób rozumienia sprowadzania treści, o jakich mowa, prezentuje również J. Warylewski (*Kodeks karny, część szczególna. Komentarz*, T. I, pod red. A. Wąska i R. Zawłockiego, C.H. Beck 2010 r. nb. 66–69 do art. 202 KK), który nadto zwraca uwagę na uchwałę Sądu Najwyższego z 14.03.1986 r. III AZP 7/85 (OSNC 1987, z. 1, poz. 1)

zawierających „treści zakazane" w systemowym koszu nie jest równoznaczne z pozbyciem się ich z komputera. Pomijając już fakt, że usunięcie plików po pewnym czasie ich posiadania jest tylko usunięciem skutków czynu i zmianą stanu istniejącego, a nie zmienia faktu popełnienia czynu w przeszłości, to, zgodnie z wyrokiem Sądu Najwyższego z 24 sierpnia 2011 r. (V KK 26/11)[363], skasowanie plików pornograficznych poprzez wrzucenie ich do kosza jest nieskuteczne i nie oznacza wyrzucenia z pamięci komputera.

gdzie wyjaśniono, że sprowadzanie obejmuje wszelkie formy wykazywania inicjatywy zmierzającej do uzyskania jakichś publikacji.
O tym, że chodzi o pozyskiwanie, działanie zmierzające do jakiejś formy dysponowania przekonuje także treść art. 202 § 3 KK, gdzie jest mowa o sprowadzaniu w celu rozpowszechniania. Aby uczynić sprowadzaną treść pornograficzną powszechnie dostępną, konieczne jest by efektem było przynajmniej ograniczone władanie treścią.
Sprowadzanie treści o jakich mowa w art. 202 § 4a KK oznaczać więc będzie wszelkie formy aktywności sprawcy zmierzające do uzyskania tych treści, spowodowania, by znalazły się dyspozycji jego lub innej osoby.
W wypadku tradycyjnych nośników, na których odwzorowane są treści pornograficzne (np. papier, płótno, płyta CD), chodzić więc będzie np. o zamawianie, otrzymywanie przesyłek z takimi treściami, przewożenie ich, wymianę. Specyfika przekazywania informacji poprzez sieć Internet polega w szczególności na pozyskiwaniu zbiorów danych bez przemieszczania realnego, posiadającego fizyczne własności przedmiotu, który je zawiera do miejsca, gdzie dana osoba (sprowadzający) go uzyskuje, zaś zapoznawanie się z takimi danymi zawartymi na stronach internetowych wymaga ich pobrania i wyświetlania na ekranie komputera użytkownika przez przeglądarkę. Jednak w tym ostatnim wypadku inicjatywa użytkownika – bo to przecież on uruchamia przeglądarkę, by dotrzeć do określonej strony internetowej nakierowana jest na to, by stronę otworzyć, wyświetlić jej zawartość i zapoznać się z nią. W wypadku samego przeglądania stron internetowych zawierających treści pornograficzne z udziałem małoletnich poniżej 15 lat, aktywność takiej osoby nie zmierza do pozyskania tych treści, spowodowania, by znalazły się w jej dyspozycji, ale do zaznajomienia się z nimi w czasie przeglądania odpowiedniej strony. Uzyskanie treści, o których mowa, wymaga dalszych czynności użytkownika zmierzających do zapisania ich na nośniku danych, by znalazły się w jego dyspozycji. Tak więc zachowanie ograniczone do wchodzenia na stronę internetową i zapoznawania się zawartymi tam przekazami pornograficznymi z udziałem małoletniego poniżej 15 lat nie stanowi sprowadzania treści o jakich mowa w art. 202 § 4a KK".

[363] Zob. K. Żaczkiewicz-Zborska: *Niedozwolony plik w koszu też jest karany*, http://www.lex.pl/czytaj/-/artykul/niedozwolony-plik-w-koszu-tez-jest-karany.

Rzeczywiście, odzyskanie takich plików jest stosunkowo łatwe, nawet dla początkującego użytkownika (opcja „przywróć")[364].

Za wysoce dyskusyjne należy uznać wprowadzenie[365] penalizacji zachowania ograniczonego do uzyskania dostępu do „informacji zakazanej" (tzw. *viewing*)[366] W chwili pisania niniejszej monografii ustawa wprowadzająca jego penalizację oczekiwała na wejście w życie, stąd też odnośnie do dwóch nowych znamion ustawowych nie może być mowy o jakiejkolwiek praktyce orzeczniczej, niemniej sama konstrukcja zmiany nasuwa szereg wątpliwości. Pornografia dziecięca staje się „informacją zakazaną" *sensu stricto*. Nasuwa się pytanie o konstytucyjność takiego tworu w świetle art. 54 ust. 1 Konstytucji RP (wolności uzyskiwania dostępu do informacji). Dotychczasowe rozwiązania dotyczące ochrony informacji (w tym informacji niejawnych) penalizowały jedynie ich ujawnienie (art. 265 KK), a nie samo uzyskanie dostępu do nich. Omawiany wcześniej art. 267 KK penalizuje wprawdzie uzyskiwanie dostępu do informacji, ale wyłącznie w pewnych szczególnych warunkach i przy wykorzystaniu pewnych sposobów. Nawet przy działalności na rzecz obcego wywiadu (art. 130 § 3 KK), karane jest gromadzenie informacji i wchodzenie do systemu informatycznego w celu zapoznania się z nią, ale nie samo uzyskanie dostępu do niej.

Drastyczny, przestępny i obrzydliwy charakter informacji nie zmienia faktu, że – gdyby oprzeć się na literalnym rozumieniu przepisu (wykładni słownikowej) – nie byłoby możliwe np. prowadzenie badań naukowych nad tego rodzaju zjawiskiem, utrudnione byłoby szkolenie zajmujących się nim specjalistów (seksuologów, psychiatrów), niemożliwe stałoby się konstruowanie narzędzi informatycznych, wyszukujących tego rodzaju infor-

[364] Mowa oczywiście nie o skasowaniu plików z pamięci buforowej przeglądarki, ale o skasowaniu uprzednio celowo zapisanych plików.

[365] Zob. np.: *Prokuratura Okręgowa w Zielonej Górze: X Seminarium Kryminalistyczne* „Kryminalistyka w Świecie Wirtualnej Zbrodni" (Jesionka, 15–17 maja 2013 r.), http://zielonagora.po.gov.pl/index.php?id=3&ida=10004.

[366] Mowa o zmianach wprowadzonych ustawą z 4 kwietnia 2014 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (dalej UzmKK). Wprowadza ona m.in. zmianę przepisów artykułu 202 KK dotyczącą penalizacji *viewingu*:

> *§ 4a. Kto przechowuje, posiada lub uzyskuje dostęp do treści pornograficznych z udziałem małoletniego, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
>
> *§ 4c. Karze określonej w § 4b podlega, kto w celu zaspokojenia seksualnego uczestniczy w prezentacji treści pornograficznych z udziałem małoletniego.*

macje np. dla celów prewencji kryminalnej czy informatyki śledczej[367] itd. Ustawodawca nie wprowadził bowiem żadnego ustawowego kontratypu czynu zabronionego. Wątpliwości może budzić nawet wejście na skompromitowaną stronę www, na której atakujący umieścił tego rodzaju treści w celu ich usunięcia – ewidentnie bowiem osoba próbująca stronę naprawić uzyska dostęp do „zakazanej treści" i to w sposób oczywiście intencjonalny (w odróżnieniu od np. odbiorcy niezamówionej przesyłki czy osoby, która na tego rodzaju treści natknęła się przypadkowo). Podobne trudności może sprawić prośba oskarżonego o prezentację inkryminowanej informacji na rozprawie czy nawet sama próba zapoznanie się sędziego z materiałem dowodowym. Z punktu widzenia biegłego pojawia się pytanie o prawną podstawę wykonania opinii (sąd nie może przecież zlecić biegłemu popełnienia przestępstwa).

Na marginesie można wspomnieć również o wątpliwościach odnośnie do art. 202 § 4c KK, gdzie mogą być poważne problemy z wykazaniem, że czyn został podjęty w celu kierunkowym, choć oczywiście będą to problemy dla śledczych i ewentualnie biegłych seksuologów, nie zaś informatyków.

Przy okazji powstaje pytanie, jak powinien zareagować użytkownik, który w sposób nieintencjonalny stał się dysponentem „informacji zakazanej", na jeden z opisanych powyżej sposobów (przypadkowe ściągnięcie z Internetu, zakup używanego nośnika itd.). Oczywiście, zgodnie z obywatelskim obowiązkiem zawiadomienia o przestępstwie (art. 304 KPK), osoba taka powinna zawiadomić o tym prokuratora lub policję[368]. Praktycznym

[367] Niektóre programy do informatyki śledczej (np. *X-ways Forensics*, http://www.x-ways.net/forensics/index-m.html) mają wbudowaną funkcję typowania zdjęć mogących zawierać treści pornograficzne (w oparciu o procentowy udział w zdjęciu kolorów zbliżonych do koloru skóry). Oczywiście istnieją współcześnie znacznie bardziej zaawansowane mechanizmy rozpoznawania obrazów (choćby wbudowane w sporą część aparatów cyfrowych mechanizmy detekcji twarzy, czy detekcji uśmiechu).

[368] W Internecie funkcjonuje również szereg tzw. punktów kontaktowych przyjmujących zawiadomienia o „nielegalnych treściach". W Polsce tego rodzaju punkty prowadzi m.in. Naukowa Akademicka Sieć Komputerowa NASK pod nazwą dyżurnet (http://www.dyżurnet.pl) czy Fundacja Orange wraz z Fundacją Dzieci Niczyje (http://helpline.org.pl). Oczywiście, działalność tego typu organizacji nie zastępuje działalności prokuratury, a zgłosze-

problemem w takim wypadku może być, uciążliwa dla powiadamiającego, konieczność zabezpieczenia procesowego śladów dowodowych (które w takim wypadku znajdują się w komputerze osoby zawiadamiającej). Należałoby dołożyć wszelkich starań, aby działania konieczne ze strony wymiaru sprawiedliwości przebiegły w sposób jak najmniej uciążliwy dla osoby zgłaszającej. Wystarczającym dla ewentualnych dalszych badań przez biegłego jest wykonanie uwierzytelnionej kopii bitowej nośnika (dysku twardego), co może zająć od kilku do kilkunastu godzin. Sytuacje, w których osoba składająca powiadomienie jest pozbawiana na dłuższy czas swojego komputera, na pewno nie powinna się zdarzać[369].

Przy okazji art. 202 KK w nowym Kodeksie karnym pojawiło się pojęcie „treści" (art. 173 KK z 1969 r. mówił wyłącznie o pismach, drukach, fotografiach lub innych przedmiotach mających charakter pornograficzny). W nowym KK ustawodawca uniknął problemów, jakie implikowałoby wykorzystanie mediów, których nośnikami są nie przedmioty, ale zjawiska fizyczne, np. fala dźwiękowa czy elektromagnetyczna, bądź osoby, np. w odniesieniu do widowisk typu *living-love*[370]. Z drugiej jednak strony, w odniesieniu do utworów literackich o charakterze pornograficznym, może pojawiać się wątpliwość, czy np. dopisanie do przeznaczonego do rozpowszechniania utworu literackiego informacji o małoletniości bohaterów (bądź o tym, że któryś z nich jest zwierzęciem) jest wystarczającym powodem do karania autora dopisku (który w ten sposób produkuje przecież treści pornograficzne z udziałem małoletniego z utworu zawierającego treści pornograficzne bez takiego udziału).

Użyte w art. 202 § 4b KK określenie „wizerunku wytworzonego albo przetworzonego" wyeliminowało wprawdzie problem słuchowisk czy opowiadań, niemniej spotkało się ze słuszną krytyką w literaturze przedmiotu[371]. Samo sformułowanie trafiło do polskiego prawa na skutek ułomnej implementacji Decyzji Ramowej Rady Europy 2004/68/WSiSW z 22 grudnia 2003 r. o zwalczaniu seksualnego wykorzystywania dzieci i pornografii dziecięcej

nie do nich ewentualnie znalezionych „zakazanych treści" nie wyczerpuje wspomnianego wyżej obowiązku powiadomienia o przestępstwie.

[369] Zob. np.: M. Frydrych, I. Kondracka: *Pomógł policji stracił komputer*, http://fakty.interia.pl/news/pomogl-policji-stracil-komputer,1439333/600bd8ff8c340a70559ecec3f70b676f.

[370] Por. J. Warylewski: *System*…, op. cit.

[371] Por. np. M. Wrześniewski: *Krytycznie*…, op. cit.

(dalej DRRESWD), która w art. 2 lit. C, pkt IV definiuje jako „pornografię dziecięcą" również „realistyczne obrazy dziecka uczestniczącego w zachowaniach o wyraźnie seksualnym charakterze lub realistyczne obrazy organów płciowych dziecka, w celach głównie seksualnych". Podobne sformułowania zawarte są także w Dyrektywie Parlamentu Europejskiego i Rady 2011/92/UE z 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (dalej DZNTCS) zastępującej wspomnianą decyzję DRRESWD.

Podobne określenie występuje też w Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych (dalej KREODSW) – art. 20 ust. 3 w brzmieniu:

„3. Każda ze Stron może zastrzec sobie prawo do wyłączenia w całości lub części stosowania ustępu 1 lit. a) oraz lit. e) w odniesieniu do produkcji i posiadania materiałów pornograficznych;

- składających się wyłącznie z udawanego przedstawiania lub realistycznych obrazów nieistniejącego dziecka;

- z udziałem dzieci, które osiągnęły wiek określony w wyniku zastosowania art. 18 ust. 2, w sytuacji, gdy obrazy te zostały wytworzone przez nie i są w ich posiadaniu za ich zgodą i wyłącznie na ich prywatny użytek".

Jak widać, w obecnej redakcji KK krajowy ustawodawca pominął określenie „realistycznego", co implikuje powstanie problemu ewentualnego karania za utwory takie, jak rysunki czy obrazy. W szczególności zaś w przypadku obrazów, na których przedstawione są postaci fikcyjne, trudno wyobrazić sobie kompetentną ocenę wieku przedstawionych postaci, np. antropomorfizowanych zwierząt czy duchów. Problem ten nie ograniczył się do akademickiej dyskusji, ale uwidocznił się już w praktyce orzeczniczej przy okazji sprawy Krzysztofa Kuszeja – malarza oskarżonego z powołanego artykułu. Jakkolwiek oskarżony został uniewinniony, to w ustnym uzasadnieniu wyroku sąd podkreślił, że „artysta musi mieć jednak świadomość, że wolność sztuki nie ma charakteru absolutnego"[372].

[372] Zob. np.: *Malarz Krzysztof Kuszej uniewinniony od zarzutu propagowania pedofilii*, http://wiadomosci.wp.pl/kat,1019395,title,Malarz-Krzysztof-Kuszej-uniewinniony-od-zarzutu-propagowania-pedofilii,wid,14791099,wiadomosc.html.

O ile odnośnie do penalizacji posiadania pornograficznych wizerunków małoletniego intencja prawodawców europejskich wydaje się dość oczywista (usunięcie z obiegu wszelkich treści pornograficznych z udziałem wizerunku małoletniego[373]), o tyle kwestia wizerunków wytworzonych bądź przetworzonych wydaje się mieć genezę raczej praktyczną, podobnie jak pkt III powołanej Dyrektywy DZNTCS, który jako pornografię dziecięcą definiuje również „wszelkie materiały ukazujące osobę wyglądającą na dziecko uczestniczącą w rzeczywistych lub symulowanych zrachowaniach o wyraźnie seksualnym charakterze oraz przedstawienia organów płciowych osób wyglądających jak dziecko, w celach głównie seksualnych"[374].

Można zastanawiać się, czy zacytowane wcześniej akty prawa europejskiego nie stanowią dobrego punktu wyjścia do wykładni systemowo-celowościowej tak nieszczęśliwie sformułowanego przepisu. Problem ten wykracza jednak zdecydowanie poza tematykę niniejszej monografii.

Zdecydowanie natomiast samo sformułowanie „wytworzonych albo przetworzonych" (bez dookreślenia „realistycznych") jest niezrozumiałe, choćby również o tyle, że raczej trudno mówić o obrazach niewytworzonych (powstałych samoistnie). Stąd też podobnych określeń należy unikać w pytaniach do biegłych, każdy bowiem obraz, film, dokument tekstowy czy zapis dźwiękowy zapisany na nośniku danych, musiał zostać uprzednio wytworzony, a już sam fakt jego digitalizacji w celu zapisania jest jakąś formą jego przetworzenia. Wątpliwości te potęguje fakt, że przy okazji penalizacji *viewingu* pominięto treści wytworzone bądź przetworzone. Z zasady racjonalnego ustawodawcy można wywodzić, że *viewing* takich treści nie jest kryminalizowany.

---

[373] Por. M. Wrześniewski: *Krytycznie…*, op. cit.

[374] Praktycznym problemem, przed którym stawały sądy, było wykazanie rzeczywistego wieku postaci w momencie wykonania zdjęcia. Zasadniczo w tym celu (jeśli nie można ustalić personaliów osoby uwidocznionej na zdjęciu czy filmie i uzyskać pewnej informacji o dacie jego powstania) wykorzystuje się opinię biegłych z zakresu antropologii. Niemniej pomiary antropometryczne wykonane na zdjęciach, czy filmach obarczone muszą być, z natury rzeczy, sporą niedokładnością. Ponadto nie można na ich podstawie rozróżnić sytuacji granicznych (czy sfotografowana osoba ukończyła piętnasty rok życia na dzień przed, czy w dzień po wykonaniu zdjęcia). Co więcej, producenci pornografii dziecięcej wykorzystywali osoby z zaburzeniami hormonalnymi, dodatkowo odpowiednio ucharakteryzowane, bądź dokonywali daleko idącego retuszu komputerowego zdjęć, ewentualnie tworzyli fotorealistyczne obrazy ukazujące postaci dzieci.

5.2 Opiniowanie w sprawach dotyczących programów komputerowych

Programy komputerowe mogą stać się przedmiotem zainteresowania wymiaru sprawiedliwości w wielu różnych okolicznościach, spośród których stosunkowo najczęstszymi są postępowania karne z art. 272 § 2 KK (uzyskanie cudzego programu komputerowego w celu osiągnięcia korzyści majątkowej bez zgody osoby uprawnionej), postępowania karne z art. 115, 116, 117 i 118 PrAut oraz postępowania cywilne dotyczące ustalenia praw autorskich do programu komputerowego.

Obowiązujące w Polsce prawo nie definiuje szeregu pojęć z zakresu inżynierii oprogramowania, w tym pojęcia „program komputerowy"[375]. Z punktu widzenia biegłego informatyka najwłaściwszym jest – podobnie jak i w innych przypadkach – przyjęcie definicji podanych w odpowiednich obowią-

[375] W wyroku składu 7 sędziów Naczelnego Sądu Administracyjnego z 24 listopada 2003 r. (FSA 2/03) sąd stwierdził: „Prawo polskie nie definiuje pojęcia »program komputerowy«, w tym nie czyni tego również ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (...). Definicji programu komputerowego nie zawiera także Dyrektywa nr 9l/250/EEC Rady Ministrów z 14 maja 1991 r. o ochronie prawnej programów komputerowych (OJ No. L.122 z 17 maja 1991 r.), gdyż uznano, że definicja przedmiotu ochrony nie jest w tym dokumencie konieczna, a jej zamieszczenie byłoby niewłaściwe ze względu na szybki postęp technologii informatycznych (A. Nowicka: *Prawnoautorska i patentowa ochrona programów komputerowych*, ABC 1995, s. 64–65). W Dyrektywie wyjaśniono jedynie, że rola programu komputerowego polega na tym, by wejść w kontakt i funkcjonować z innymi częściami składowymi systemu komputerowego i użytkownikami.
W doktrynie oraz uregulowaniach prawnych innych państw program komputerowy określany jest najczęściej jako zakodowana sekwencja instrukcji (rozkazów) wykonywanych bezpośrednio lub pośrednio przez komputer albo inne urządzenie zdolne do przetwarzania informacji w celu uzyskania określonego rezultatu (realizacji określonych funkcji i zadań). W niektórych definicjach zaznacza się, że program »stanowią takie sekwencje symbolicznych instrukcji lub komunikatów, które mogą być w sposób automatyczny przetworzone na zakodowane sekwencje instrukcji« (J. Sobczak: *Prawo autorskie i prawa pokrewne*, Iuris 2000, s. 167–168).
Tak pojmowany program komputerowy – jako celowy zbiór określonych instrukcji – ma jednak zawsze charakter dobra niematerialnego, niezależnie od tego, czy jest utworem, czy też nie jest utworem w ujęciu prawa autorskiego". Zob. też G. Borkowski: *VAT od sprzedaży programów komputerowych*, „Glossa" Nr 03/2004, http://www.czasopisma.pwp.pl/glosa-200403.xml?katalog=2004038.

zujących Polskich Normach, a jeśli to możliwe – również przekonanie sądu i stron do używania definicji z Polskich Norm, bowiem w sprawach sądowych precyzja wypowiedzi jest szczególnie wskazana[376]. I tak:

- ✓ pojęcie „program komputerowy" definiuje się w Polskiej Normie jako „jednostkę syntaktyczną zgodną z zasadami konkretnego języka programowania, składającą się z deklaracji i instrukcji lub rozkazów potrzebnych do rozwiązania funkcji, zadania lub problemu"[377];
- ✓ „programowanie" (czyli według definicji normatywnej „projektowanie, zapisywanie, modyfikowanie i testowanie programów"[378]) jest określeniem czynności tworzenia programu komputerowego, przy czym tradycyjnie używa się w języku polskim wyrażenia „pisać programy", które jest pewnym archaizmem, pochodzącym z czasów, kiedy czynność programowania polegała na fizycznym zapisaniu określonego algorytmu w pewnym języku programowania (język programowania jest definowany jako „język sztuczny służący do tworzenia programów"[379]). Współczesne narzędzia programistyczne (generatory kodów[380]) pozwalają graficzne projektować np. interfejs programu i wygenerować obszerne fragmenty kodu źródłowego za pomocą odpowiednich kreatorów.
- ✓ złożoność współczesnych programów powoduje, że – inaczej niż miało to miejsce w przypadku stosunkowo niewielkich i mało skomplikowanych programów sprzed kilku lat – poszczególne ich części umieszczane są w kilku lub kilkunastu plikach dyskowych. Do dość powszechnych należy sytuacja, w której różne

[376] Nieprecyzyjny język uczestników postępowań sądowych może powodować niezrozumienie istoty problemu zarówno przez sąd, jak i przez biegłego (np. pojęcia „platformy", czy „systemu", które pojawią się w wypowiedziach prawników jako synonimy „oprogramowania" mogą sugerować, że zadawane pytania czy stawiane tezy dotyczą również sprzętu komputerowego).

[377] PN-ISO/IEC 2382-1:1996 – 01.05.01. Warto zwrócić uwagę, że trzymając się ściśle języka norm o programie komputerowym mowa w odniesieniu do kodu źródłowego.

[378] PN-ISO/IEC 2382-1:1996 – 01.05.03.

[379] PN-ISO/IEC 2382-1:1996 – 01.05.10.

[380] „Podprogram, często część kompilatora, który przekształca całość lub część programu napisanego w pewnym języku pośrednim na język wynikowy" PN-ISO/IEC 2382-7:2002 – 07.04.42.

programy docelowe[381] wywołują się wzajemnie albo korzystają ze wspólnych fragmentów kodu umieszczonych w różnych bibliotekach czy modułach tworzonych, bądź na poziomie programu źródłowego (dołączanie statyczne), bądź też na poziomie kodu wynikowego (biblioteki dołączane dynamicznie, ang. *Dynamic Link Libraries*);

- ✓ „oprogramowanie" definiowane jest jako „wszystkie lub niektóre programy, procedury, reguły i związana z tym dokumentacja systemu przetwarzania informacji"[382]. W skład tak rozumianego oprogramowania, oprócz programów, można – jak się wydaje – zaliczyć również wyodrębnione w postaci osobnych plików dyskowych inne składniki, takie jak definicje czcionek i krojów pisma, pliki pomocy (ang. *help*), dodatkowe pliki tekstowe zawierające instrukcję obsługi programu, bądź jej fragmenty i inne. W szczególności oprogramowanie może być dystrybuowane razem z plikami, na których ma wykonywać operacje, w tym z bazami danych;
- ✓ według Polskiej Normy baza danych[383] jest to „zbiór danych zorganizowany zgodnie z pojęciową strukturą opisującą charakterystyki tych danych oraz związki między ich odpowiednimi elementami, stosowany w jednym lub wielu zastosowaniach"[384]. Nazywa się w ten sposób ogólnie wszelkie ustrukturalizowane zbiory informacji (tj. zawierające informacje o podobnej budowie). W przypadku systemu komputerowego bazy danych przechowywane są w odpowiednich strukturach danych w pamięci masowej, a więc odpowiadają im pliki dyskowe lub katalogi (foldery) o określonej strukturze.

[381] „Program docelowy – przetłumaczona wersja programu źródłowego" PN-ISO/IEC 2382-7:2002 – 07.04.51.

[382] PN-ISO/IEC 2382-1:1996 – 01.01.8.

[383] Warto przypomnieć (por. przypis 316), że inną definicje bazy danych zawiera art. 2. UOBD: „baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości".

[384] PN-ISO/IEC 2382-1:1996 – 01.08.05.

> Bazę danych należy odróżnić od systemu zarządzania bazami danych (SZBD, ang. *Database Management System*, DBMS), przez który zazwyczaj rozumie się oprogramowanie służące do przetwarzania informacji zawartej w bazach danych i od języków programowania tego rodzaju systemów (języków tworzenia systemów zarządzania bazami danych)[385].

W ustawie PrAut, programy komputerowe wymienione są jako rodzaj dzieł podlegających ochronie (art. 74 ust. 1), przy czym art. 1 ust. 1 powołanej ustawy określa jako dzieła te spośród wytworów ludzkich, które stanowią przejaw działalności twórczej i mają indywidualny, niepowtarzalny charakter (a zatem spełniają warunki zarówno nowości subiektywnej, jak i obiektywnej), przy czym bez znaczenia jest charakter programu. Autorstwa dzieła nie można bowiem rozpatrywać w kategoriach jego jakości czy kunsztu twórcy ani też znaczenia, rozmiarów, funkcji, czy wartości opracowanych fragmentów[386]. Należy wspomnieć o obecnych w literaturze

[385] Por. M. Szmit: *Informatyka*…, op. cit., s. 68 i nast. Niestety, dość często w mowie potocznej, mówi się po prostu o „bazach danych", co utrudnia zrozumienie problemu przez osoby nie będące informatykami, stąd należy w tym miejscu podkreślić konieczność precyzyjnego wyrażania się (nawet jeśli skutkuje to wzrostem objętości opinii).

[386] Zob. np.: Z. Okoń: *Komputerowe paragrafy – Program komputerowy w prawie autorskim*, „PCkurier" Nr 13/1998: „Nie należy też mylić programu komputerowego ze spełnianą przezeń funkcją. Nie można powoływać się na brak oryginalności np. edytora tekstów, który funkcjonalnie jest identyczny z innym. Prawo autorskie chroni bowiem formę utworu, którą w przypadku programu komputerowego jest przede wszystkim jego kod, zapisany w jakimś języku programowania. Raczej mało prawdopodobne jest, aby dwóch programistów rozwiązujących jakiś bardziej obszerny problem napisało identyczne programy. Z tych też względów twórca programu nie musi się wykazać przy programowaniu żadnymi większymi umiejętnościami, a rezultat jego pracy, nawet nieudolny, może być chroniony przez prawo autorskie. Swego czasu w doktrynie niemieckiego prawa autorskiego uważano, że aby program mógł być uznany za oryginalny i tym samym mógł być chroniony przez prawo autorskie, jego twórca powinien wykazać się umiejętnościami programistycznymi przekraczającymi przeciętną. Z podejścia takiego jednak zrezygnowano, ponieważ okazało się, że przy przyjęciu takiego restrykcyjnego kryterium prawie 80-proc. programów rozpowszechnianych na niemieckim rynku byłoby pozbawionych ochrony. (…) jedną z podstawowych zasad prawa autorskiego jest ochrona formy utworu, a nie idei w nim wyrażonych. Zasadę tę prawo autorskie podkreśla jeszcze raz już w odniesieniu do programów komputerowych. Zasada swobodnego dostępu do idei wyrażonych w utworze przy jednoczesnej ochronie jego formy ma na celu z jednej strony umożliwienie swobodnego rozwoju nauki czy sztuki, a z drugiej zapewnienie twórcy utworu godziwego wynagrodzenia za jego pra-

prawniczej tendencjach negowania twórczego charakteru programów komputerowych. Często używanym argumentem jest to, że funkcjonalny charakter programów komputerowych ogranicza bądź wręcz eliminuje swobodę twórczą, narzucając jedyne możliwe ich ukształtowanie, czego efektem jest ograniczenie, a nawet wyłączenia ochrony prawnoautorskiej[387].

Jest to stanowisko z punktu widzenia informatyka często niezrozumiałe: o takiej sytuacji można byłoby mówić wyłącznie w przypadku, gdyby programista wykonywał jedynie czynności techniczne, mechaniczne, rutynowe (np. dostarczanie materiałów, informacji, finansowanie prac itd.[388]). Prace wykonywane przez tego rodzaju pracowników mają bowiem charakter jedynie pomocniczy, niezwiązany z zasadniczą działalnością twórczą, albo też gdyby programiście nie przysługiwała żadna swoboda w sposobie programowania: projektant przedstawiłby mu nie tylko specyfikację wymagań odnośnie do funkcji wykonywanych przez program czy jego fragment, ale również narzucił sposób ich realizacji, wykorzystanie konkretnych struktur danych, instrukcji języka programowania, ścisły wygląd interfejsu użyt-

cę. Prawo autorskie za idee uważa między innymi koncepcje artystyczne, metody zastosowane przy tworzeniu dzieła, styl czy manierę artysty, jak również teorie naukowe, systemy ekonomiczne, prawne, polityczne, przepisy kucharskie, zasady gier, metody promocji i kampanii reklamowej. Idee zawarte w programie komputerowym to przede wszystkim spełniana przez program funkcja, algorytm (rozumiany jako sposób rozwiązania danego problemu), zasady komunikacji ze sprzętem, innymi programami czy użytkownikiem (interfejsy nazywane przez ustawę »łączami«). Ustawa o prawie autorskim i prawach pokrewnych dodatkowo podkreśla wyłączenie spod ochrony idei i zasad właśnie w odniesieniu do programu komputerowego (art. 74 ust. 2 zd. 2). Zasadą jest też, że prawo autorskie chroni tylko te elementy dzieła, które są oryginalne. Jeżeli więc oryginalność jakiegoś utworu, w tym i programu komputerowego, mieści się jedynie w zakresie idei w nim wyrażonych, natomiast forma pozbawiona jest tej cechy – utwór nie będzie chroniony. Jednocześnie z zasady tej wynika, że chroniony może być dowolnie krótki fragment utworu, jeżeli tylko jest oryginalny".

[387] Zob. J. Barta [w:] *System prawa prywatnego. Prawo autorskie*, Tom 13, pod red. Z. Radwańskiego, Warszawa 2007, s. 859–860.

[388] Wg L. Widmański: *Programy komputerowe i bazy danych jako samodzielne dobra na gruncie prawa polskiego – w szczególności w kontekście Internetu. Wybrane zagadnienia*, praca magisterska napisana na Wydziale Prawa i Administracji Uniwersytetu Śląskiego w Katowicach, http://vagla.pl/skrypts/mgr_l_widmanski.pdf, s. 16 i nast.

kownika itd. Można spodziewać się, że istnieje pewna liczba programów niebędących utworami w sensie prawa autorskiego, a zatem niepodlegających ochronie prawnoautorskiej.

Ochronie prawnoautorskiej podlega forma utworu, którą w przypadku programu komputerowego jest kod wyrażony w języku programowania (z uwzględnieniem tego, co powiedziano wcześniej o współczesnych narzędziach programowania wizualnego i generatorach kodów). Ustawodawca zdecydował o wyłączeniu spod ochrony idei i zasad będących podstawą jakiegokolwiek elementu programu komputerowego. Za pozbawione twórczego charakteru uznaje się w literaturze prawniczej języki programowania (choć sygnalizuje się sporadyczną możliwość ich ochrony), interfejsy są zaliczane do elementów chronionych, ale w sposób ograniczony, ze względu na techniczne wymagania przy ich opracowywaniu, z kolei algorytmy traktuje się jako elementy przedmiotowo istotne, decydujące o twórczym znaczeniu całego programu komputerowego[389], ale same jako takie niepodlegające ochronie prawnoautorskiej. O twórczym charakterze programu komputerowego decyduje posiadanie cechy nowości w znaczeniu obiektywnym w odniesieniu do co najmniej jednego z jego elementów mogących podlegać twórczemu kształtowaniu. W konsekwencji pierwszym zagadnieniem, z którym styka się sąd przy rozpatrywaniu spraw, w których istotną rolę pełnią prawa autorskie do programów komputerowych, jest konieczność rozstrzygnięcia, czy program, ewentualnie jego fragment, o którym mowa ma charakter utworu w sensie prawnoautorskim i czy w związku z tym jego twórcom przysługują prawa autorskie do niego. Pytania kierowane do biegłego informatyka w takim wypadku mogą być trudno zrozumiałe i wymagać dość wnikliwej analizy, bowiem – jak powiedziano powyżej – prawnicy mają, dla informatyków trudno zrozumiałą, tendencję do negowania twórczego charakteru działalności programistów, a ponadto przepisy i orzecznictwo odnośnie do prawa autorskiego są jednymi z bardziej skomplikowanych. W szczególności fakt, że inżynieria oprogramowania popiera i rozwija metody wielokrotnego wykorzystania kodu, bywa podnoszony przez prawników jako argument za nietwórczym charakterem programów komputerowych. Dla informatyka jest to argument o tyle mało przekonywujący, że i w innych dziedzinach ludzkiej

[389] Zob. R. Golat: *Prawo autorskie i prawa pokrewne*, C.H. Beck, Warszawa 2006, s. 69 i nast.

twórczości dochodzi do wielokrotnego wykorzystania tych samych elementów składowych (w muzyce: akordów i kadencji, w zdobnictwie: motywów charakterystycznych dla danej kultury, w książkach prawniczych licznych cytowań z innych autorów, orzecznictwa i aktów prawnych itd.) i nikt nie neguje z tego powodu twórczego charakteru takich utworów. Być może źródłem nieporozumienia jest zapis art. 74 ust. 1 PrAut, który zawiera *explicite* stwierdzenie, że programy komputerowe podlegają ochronie jak utwory literackie, zaś oczywiście twórczy charakter utworu literackiego, który wykorzystywałby w przytłaczającej większości swojej zawartości cytaty z innych utworów, mógłby być wątpliwy[390].

[390] Choć nie zawsze, również dlatego, że także kompilacyjny charakter dzieła nie uniemożliwia uznania go za utwór w rozumieniu art. 1 PrAut. Mówi o tym wyrok Sądu Najwyższego z 25 stycznia 2006 r. (I CK 281/05): „Syntetyczna definicja utworu zawarta jest w art. 1 ust. 1 PrAut; jest to każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia. Wskazana definicja w sposób generalny określa więc cechy konieczne wyróżniające utwór od innych rezultatów działalności człowieka. Przy rozstrzyganiu kwestii, czy dany rezultat pracy korzysta z autorskoprawnej ochrony sądy często posługują się wskazówkami wypracowanymi w orzecznictwie, w szczególności Sądu Najwyższego. W dotychczasowym orzecznictwie za przedmiot prawa autorskiego uznano m.in. kolekcje afiszy lub ogłoszeń, katalogi, rozkłady kolejowe, książki kucharskie, wzory i formularze, kompozycje z kwiatów, projekty dokumentacji technicznej, wzór zdobniczy lub projekt znaku towarowego. Na uwagę zasługuje wyrok Sądu Najwyższego z 5 marca 1971 r. (I CR 593/70), w którym m.in. stwierdzono, że o powstaniu prawa autorskiego nie decyduje stopień wartości opracowanego dzieła, gdyż nawet znaczeniowo niewielkie opracowania mogą stanowić przedmiot ochrony autorskiej, byleby cechował je element twórczości autora.
Oceniając więc spełnienie wymagań stawianych utworom w rozumieniu art. 1 ust. 1 PrAut, należy brać pod uwagę całość cech w ich konkretnym, oryginalnym zestroju. Nie stanowi przeszkody w uznaniu za utwór okoliczność, że wykorzystano w nim elementy ogólnie dostępne. Jako takie elementy nie są objęte ochroną, gdyż utworem może być kompilacja powszechnie dostępnych danych, byleby sposób doboru, segregacji, ujęcia lub przedstawienia tych danych miał znamiona oryginalności. Wynika to wyraźnie z art. 3 PrAut. Charakter twórczy jako immanentna cecha utworu w rozumieniu art. 1 ust. 1 PrAut jest przejawem intelektualnej działalności człowieka, jakkolwiek nie każdy proces intelektualny prowadzi do powstania rezultatu o cechach twórczych. Praca intelektualna o charakterze twórczym jest przeciwieństwem pracy o charakterze technicznym, która polega na wykonywaniu czynności wymagających jedynie określonej wiedzy i sprawności oraz użycia określonych narzędzi, surowców i technologii. Cechą pracy w charakterze technicznym jest przewidy-

Kolejną trudnością, którą należy wziąć pod uwagę przy omawianiu kwestii prawnoautorskich jest różnica pomiędzy rozumieniem, jakie pojęciu „utwór" nadaje PrAut, a rozumieniem potocznym, w tym zasadami niektórych etyk szczegółowych (np. etyki naukowej), w której przyjmuje się zazwyczaj że udział w stworzeniu koncepcji wystarcza do uznania kogoś za współautora dzieła[391], podczas kiedy PrAut nie chroni idei, w szczególności idei zawartych w programie komputerowym. Opiniując w sprawach dotyczących praw autorskich do programów komputerowych należy mieć na względzie powyższe uwarunkowania, pamiętając jednocześnie, że nie jest rolą biegłego pouczanie sądu o stanach prawnych.

walność i powtarzalność osiągniętego rezultatu. Proces tworzenia, w przeciwieństwie do pracy technicznej, polega na tym, że rezultat podejmowanego działania stanowi projekcję wyobraźni osoby, od której pochodzi, zmierzając do wypełniania tych elementów wykonywanego zadania, które nie są jedynie wynikiem zastosowania określonej wiedzy, sprawności, surowców, urządzeń bądź technologii. W tym ujęciu twórczość, jako angażująca wyobraźnię twórcy, ma charakter subiektywny. Tak rozumiana twórczość powinna być odróżniona od podobnego znaczenia używanego w sferze własności przemysłowej, np. w odniesieniu do wynalazków. Twórczość jest tu bowiem pojmowana w sposób zobiektywizowany i oparty na kryterium wartości w ustaleniu określonej prawidłowości, zależności lub cech. Twórczością w zakresie wynalazków będzie np. dokonanie wynalazku w znaczeniu sformułowania nowej, czyli wcześniej nieznanej i nadającej się do zawodowego lub komercyjnego zastosowania procedury prowadzącej do osiągnięcia określonego rezultatu produkcyjnego.

Wymaganie nowości nie jest natomiast niezbędną cechą twórczości jako przejawu intelektualnej działalności człowieka. Jak wskazano, utworem może być nawet kompilacja wykorzystująca dane powszechnie dostępne pod warunkiem, że ich wybór, segregacja, sposób przedstawienia ma znamiona oryginalności".

[391] „Minimalne kryterium współautorstwa stanowi udział w stworzeniu koncepcji badań, ich przeprowadzeniu, interpretacji lub przygotowania publikacji w obszarze specjalności współautora, co najmniej w takiej części, która wystarcza do tego aby podjął on za nią publiczną odpowiedzialność" (*Stanowisko Zespołu ds. Etyki w Nauce z 16 listopada 2000 r.*, Komitet Badań Naukowych, http://kbn.icm.edu.pl/etyka/praktyka.html). Podobnie formułuje tę kwestię Kodeks etyki pracownika naukowego PAN, który w punkcie 4.1.3 stwierdza „Plagiatowanie polega na przywłaszczeniu cudzych idei, wyników badań lub słów bez poprawnego podania źródła, co stanowi naruszenie praw własności intelektualnej" (Kodeks etyki pracownika naukowego PAN przyjęty 13 grudnia 2012 r. przez Zgromadzenie Ogólne PAN, http://www.instytucja.pan.pl/images/stories/pliki/Komisja_ds_Etyki_Nauce/dokumenty/Kodeks_etyki_pracownika_naukowego_31.12._2012.pdf).

Z programami komputerowymi wiąże się zagadnienie jednej z form tzw. piractwa komputerowego[392] – czynu penalizowanego z art. 278 § 2 KK

Art. 278.

§ 1. Kto zabiera w celu przywłaszczenia cudzą rzecz ruchoma, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. Tej samej karze podlega, kto bez zgody osoby uprawnionej uzyskuje cudzy program komputerowy w celu osiągniecia korzyści majątkowej.

§ 3. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 4. Jeżeli kradzież popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

§ 5. Przepisy § 1, 3 i 4 stosuje się odpowiednio do kradzieży energii lub karty uprawniającej do podjęcia pieniędzy z automatu bankowego.

Warto zwrócić uwagę na dwa szczegóły konstrukcji tego przepisu:

- ✓ cel kierunkowy;
- ✓ pojęcie zgody osoby uprawnionej.

W odniesieniu do celu kierunkowego trzeba zauważyć, że w literaturze przedmiotu rozpowszechniona jest opinia, że już samo „nielegalne uzyskanie" programu komputerowego wiąże się z korzyścią majątkową w postaci nieponiesienia wydatków na jego (legalne) nabycie[393]. Z drugiej

[392] Kwestie związane z nielegalnym rozpowszechnianiem utworów, w tym programów komputerowych, reguluje głównie PrAut. Zob. np.: M. Szmit, A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec: *Elementy*…, op. cit., s. 89 i nast.

[393] Zob. np.: J. Curyło: *Przestępstwa przeciwko mieniu (art. 278 – art. 294 KK)*, Szkoła Policji w Pile, Piła 2011, http://isp.policja.pl/download/12/1537/przeciwkomieniu.pdf, s. 10: „Korzyścią majątkową osiągniętą w wyniku nielegalnego skopiowania programu komputerowego na tzw. własny użytek jest uzyskanie możliwości korzystania z tego programu bez ponoszenia wydatków związanych z jego legalnym nabyciem". Taką samą opinię prezentują np. A. Adamski (*Prawo*…, op. cit., s. 104), K. Gienias (K. Gienias: *Dystrybucja kopii utworów za pomocą aplikacji peer to peer (P2P)*, „Prokurator" Nr 4/2005, s. 72–79, http://www.sprp.com.pl/tresc/prokurator/6da368d4e4c3ed60007775cf200ace37.pdf), czy M. Sowa (M. Sowa: *Ogólna charakterystyka przestępczości internetowej*, „Palestra" Nr 5/6/2001, s. 25).

strony, podnoszony jest argument, że kradzież i późniejsze dysponowanie rzeczą jak właściciel z natury rzeczy powoduje wzrost aktywów sprawcy przestępstwa, a więc w stanowiącym znamię czasownikowe „uzyskaniu" mieści się korzyść majątkowa wynikająca z niezapłacenia ceny programu, *ergo*: znajdujących się w dyspozycji artykułu słów „w celu osiągnięcia korzyści majątkowej", nie można – zgodnie z zasadą racjonalności ustawodawcy – interpretować jako nadmiarowych[394]. Powstaje zatem pytanie, czy istnieją sytuacje, w których takie (bez zgody osoby uprawnionej) uzyskanie programu może nie wiązać się z tak rozumianą korzyścią majątkową? Można sobie wyobrazić uzyskiwanie w ten sposób („nielegalną drogą") programu, który pozostaje dla uzyskującego bezpłatny[395]. Praktyka orzecznicza jest we względzie karalności programów zdobytych do celów niekomercyjnych niejednolita, choć raczej należy się spodziewać interpretacji restrykcyjnej, szczególnie jeśli mowa o dużej liczbie programów o znacznej wartości rynkowej.

Odnośnie do zgody osoby uprawnionej, to warto przypomnieć (por. uwagi o ustawowym znamieniu sprowadzania – rozdział 5.1), że posiadanie programu komputerowego bez żadnych dowodów świadczących o prawnie dopuszczalnym sposobie jego zdobycia nie jest samo w sobie równoważne zdobyciu go bez zgody osoby uprawnionej. Licencje udzielane są na użytkowanie programów komputerowych, nie ma obowiązku uzyskania licencji na ich zakup (zakup programu nie wymaga zgody osoby uprawnionej). Rozpatrywanie pojęcia „zgody osoby uprawnionej" może być sensowne w kontekście uzyskiwania praw do programu przez – na przykład – prawnego następcę jego nabywcy, albo przez biegłego, który

[394] W tym kontekście często przywoływany jest wyrok Sądu Apelacyjnego w Lublinie z 10 lipca 2003 r. (II Aka 107/03), w którym Sąd stwierdził m.in.: „przy przestępstwach kradzieży kwalifikowanej, motywacja »z chęci zysku« należy do istoty tych przestępstw", w wyroku tym chodziło jednak o niemożliwość uznania takiej motywacji za zasługującą na szczególne potępienie, a nie o twierdzenie, że w znamieniu „uzyskuje" mieści się już korzyść majątkowa.

[395] Z własnych doświadczeń autora można przywołać przypadek, w którym student uczelni, która miała podpisaną umowę partnerską z dystrybutorem oprogramowania, umożliwiającą nieodpłatne korzystanie przez studentów tejże uczelni z komercyjnych wersji programów, pozyskiwał te programy – choć wydaje się to być działanie pozbawione głębszego sensu – w wersji „skrakowanej" z pirackich serwerów. Można też rozważać zdobywanie w ten sposób programu, na użytkowanie którego osoba uzyskująca program posiada licencję, a który został z jakichś powodów wycofany z dystrybucji.

zgodnie z postanowieniem sądu wykonuje kopię oprogramowania np. w celu przeprowadzenia przez sąd eksperymentu procesowego (nie jest oczywiście wówczas ani zobowiązany do zakupu dodatkowej licencji na koleje stanowiska, ani nie popełnia przestępstwa z omawianego artykułu). Nie ma też – przynajmniej, jeśli mowa o osobach fizycznych, nieprowadzących działalności gospodarczej – obowiązku przechowywania poświadczeń („dowodów legalności") uzyskania posiadanych aktywów, czy będą to przedmioty codziennego użytku, czy programy komputerowe, tak jak nie ma obowiązku legitymowania się nimi na wezwanie policji czy prokuratury. Natomiast nabywanie nielegalnych kopii programów, bądź nabywanie kopii programów niewiadomego pochodzenia, w okolicznościach które świadczą lub mogą świadczyć o ich nielegalnym pochodzeniu jest czynem kryminalizowanym w art. 291 i 292 KK (odpowiednio paserstwo umyślne i nieumyślne)

> ***Art. 291.***
>
> *§ 1. Kto rzecz uzyskaną za pomocą czynu zabronionego nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
>
> *§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.*
>
> ***Art. 292.***
>
> *§ 1. Kto rzecz, o której na podstawie towarzyszących okoliczności powinien i może przypuszczać, że została uzyskana za pomocą czynu zabronionego, nabywa lub pomaga do jej zbycia albo tę rzecz przyjmuje lub pomaga do jej ukrycia, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.*
>
> *§ 2. W wypadku znacznej wartości rzeczy, o której mowa w § 1, sprawca podlega karze pozbawienia wolności od 3 miesięcy do lat 5.*
>
> ***Art. 293.***
>
> *§ 1. Przepisy art. 291 i 292 stosuje się odpowiednio do programu komputerowego.*

§ 2. Sąd może orzec przepadek rzeczy określonej w § 1 oraz w art. 291 i 292, chociażby nie stanowiła ona własności sprawcy.

Kolejną kwestią jest zagadnienie użytkowania programu po upływie czasu ważności licencji (a więc np. przedłużone korzystanie z wersji *trial*); w tym wypadku nie może być mowy o „nielegalnym uzyskaniu" (trudno uznać, że po upływie okresu licencyjnego następuje ponowne, tym razem już „nielegalne" uzyskanie programu). Trudności powstają też w przypadku, gdy zmianie uległy warunki, na jakich została udzielona licencja (np. użytkowanie legalnie nabytej wersji „dla małych przedsiębiorstw" w sytuacji, gdy przedsiębiorstwo rozwinęło się na tyle, że przestało spełniać wymogi licencyjne). W takich wypadkach może ewentualnie znajdować zastosowanie art. 115 ust. 3 PrAut, choć należy pamiętać o zastrzeżeniach podnoszonych odnośnie do jego nieokreśloności (zob. przypis 327). Można wreszcie rozważać również, wspomniane wcześniej wykroczenie szalbierstwa.

Powyższe rozważania dotyczą strony prawnej, która nie jest – a przynajmniej nie powinna być – przedmiotem zainteresowania biegłych, mogą natomiast wyjaśnić, dlaczego – obecny zarówno w języku prasowym, jak i niestety w postanowieniach organów procesowych – głęboko niewłaściwy związek frazeologiczny „nielegalne oprogramowanie" powinien zdecydowanie zostać z języka prawniczego i – co z punktu widzenia niniejszej monografii bardziej istotne – języka biegłych zdecydowanie wyeliminowany.

5.3 Opiniowanie w sprawach cywilnych[396]

Do postępowania cywilnego w sensie materialnym zalicza się sprawy wynikające ze stosunków: prawa cywilnego, rodzinnego i opiekuńczego oraz prawa pracy. Szczególnie ważną z punktu widzenia biegłego cechą postępowania procesowego w sprawach cywilnych jest większe niż w procesie karnym[397] znaczenie zasady kontradyktoryjności[398]. Konsekwencją tego

[396] Wykorzystano fragmenty artykułu M. Szmit: *Biegły informatyk w postępowaniu cywilnym*, „Zeszyty Naukowe Politechniki Łódzkiej", seria „Elektryka" z. 121, Nr 1078, s. 487–501, Łódź 2011.

[397] Na lipiec 2015 r. przewidziana jest nowelizacja procedury karnej (ustawa z 27 września 2013 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw podpisana przez Prezydenta 17 października 2013 r.) zakładająca m.in. przemodelowanie

stanu rzeczy może być ograniczenie aktywności biegłego, który – w odróżnieniu od procedury karnej – nie ma możliwości sugerowania uzupełnienia materiału dowodowego czy przeprowadzenia dodatkowych badań[399] (nawet zresztą sąd w postępowaniu cywilnym może – choć nie musi – poprzestać na „prawdzie" formalnej, a więc – mówiąc w uproszczeniu – obrazie faktów wynikającym z domniemania prawnego lub z przyjętych zgodnie

postępowania sądowego w kierunku większej kontradyktoryjności oraz zaktywizowanie stron procesowych przy jednoczesnym wzmocnieniu roli sądu jako arbitra. Jakkolwiek w chwili obecnej nie bardzo jeszcze wiadomo, w jaki sposób będzie kształtowała się praktyka procesowa po wejściu w życie tej ustawy, wydaje się, że przynajmniej niektóre spostrzeżenia odnośnie do opiniowania w postępowaniu cywilnym będą mogły być użyteczne w nowej procedurze karnej.

[398] W piśmiennictwie zawierającym praktyczne porady odnośnie do procesów cywilnych można znaleźć daleko idące interpretacje takiego stanu rzeczy, mianujące strony gospodarzami postępowania sądowego (np. w tekście Wielkopolska Grupa Prawnicza: *Opinia biegłego pozasądowego w procesie cywilnym*, http://www.wgpr.pl/publikacje/77-opinia-bieglego-pozasadowego-w-procesie-cywilnym.html, autorzy piszą wręcz: „Polskie postępowanie cywilne zostało ukształtowane jako postępowanie kontradyktoryjne, czyli postępowanie, w którym obowiązek zgromadzenia materiału dowodowego niemal w całości spoczywa na stronach. W myśl zasady kontradyktoryjności to strona jest gospodarzem procesu, natomiast rola sądu sprowadza się do oceny tego, co zaoferują strony tak w zakresie faktów, jak i dowodów na ich poparcie"). W rzeczywistości gospodarzem postępowania sądowego jest sąd [Zob. np.: Wyrok Trybunału Konstytucyjnego z 11 września 2007 r. (P 11/07), Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 12 maja 2008 r. (II SA/WA 326/08)], który również w postępowaniu cywilnym ma inicjatywę dowodową m.in. w zakresie powoływania biegłych (art. 278 § 1 KPC) i zarządzania z ich udziałem oględzin (art. 292 KPC). Ewentualną różnicą, odnośnie do roli biegłego, o której można by dywagować, pomiędzy KPK a KPC jest to, że KPC nie przewiduje – inaczej niż ma to miejsce w KPK (art. 202 § 2) – inicjatywy dowodowej biegłych, ale dotyczy to, nieinteresującej z punktu widzenia tej monografii, roli biegłych psychiatrów.

[399] Jak piszą P. Kowalski i J. Składzień: „Pierwszą istotną rzeczą, którą powinien wiedzieć biegły jest to, że nie dysponuje on swobodą formułowania żądań, co do materiału dowodowego wykraczającego poza wnioskowany przez strony dla wydania opinii (…). Biegły w sporze cywilnym musi być świadom, iż dla wydania swojej opinii dysponuje tylko i wyłącznie tym, co zawnioskowały strony sporu". Zob. P. Kowalski, J. Składzień: *Opiniowanie w sprawach cywilnych i karnych jako problem w praktyce biegłego*, „Otorynolaryngologia" Nr 3(3)/2004.

przez strony ustaleń)[400]. Szczególnie drażliwe jest to w sytuacji, w której materiał dowodowy jest niewystarczający do wyciągnięcia wniosków, a mógłby być stosunkowo łatwo uzupełniony. Uwidacznia się w takich sytuacjach zasadnicza różnica pomiędzy postępowaniem karnym – z dominującą zasadą prawdy materialnej, która pozwala biegłemu na – w zasadzie swobodne – formułowanie postulatów odnośnie do uzupełnienia materiału dowodowego, a postępowaniem cywilnym, w którym każda ze stron dowodzi swoich tez w sposób, jaki uznaje za stosowny i realizuje to na miarę swoich możliwości i umiejętności[401].

Oczywiście nie oznacza to, aby biegły miał prawo mijać się z prawdą (materialną) tylko dlatego, że strony sporu sądowego zgodnie twierdzą coś,

[400] Zob. uchwała Izby Cywilnej SN z 17 lutego 2004 r. (III CZP 115/03): „w doktrynie powstał problem dotyczący obowiązywania zasady prawdy materialnej; w szczególności po skreśleniu art. 3 § 2 i zmianie art. 232 KPC uzasadnione stało się pytanie, czy ustawodawca odstąpił od zasady prawdy materialnej, określanej poprzednio jako »prawda obiektywna«, na rzecz prawdy formalnej. Odpowiedź na to pytanie należy do nauki prawa procesowego, która – w publikowanych dotychczas głosach – opowiada się za tezą, że jakkolwiek ograniczono instrumenty prawne pozwalające sądowi na dotarcie do prawdy, jak też przeniesiono ciężar dochodzenia do niej na strony, to jednak, zważywszy zwłaszcza na obowiązywanie art. 3, 212, 213 § 1, art. 229, 232 zdanie drugie i 339 § 2 KPC, zasada prawdy materialnej nadal obowiązuje, samo zaś dochodzenie do prawdy może być poczytywane jako jeden z celów procesu sądowego. Tezę tę trzeba uznać za trafną, bez wątpienia jednak zasada prawdy materialnej nie ma współcześnie charakteru bezwzględnego, ustawodawca bowiem wielokrotnie ogranicza ją lub koryguje (np. art. 231, 234, 233 § 2, art. 246, 247 i 217 § 2). Ograniczenie funkcjonowania tej zasady dyktowane jest różnymi motywami; ustawodawca albo chroni w ten sposób określone wartości (np. w zakresie prawa rodzinnego) albo realizuje pożyteczne społecznie cele (np. przyspieszenie i uproszczenie postępowania). Innymi słowy, ustawodawca, nie rezygnując z podstawowego celu procesu, jakim jest dojście do prawdy materialnej, pozwala w wielu przypadkach na poprzestanie na prawdzie formalnej. Dzieje się tak również wtedy, gdy wszystkie narzędzia pozwalające odkryć prawdę pozostają w rękach stron, które jednak – z różnych powodów – z nich nie korzystają bądź czynią to nieumiejętnie". Zob. też A. Kallaus: *Konsekwencje prawne zmiany przepisu art. 3 KPC w postępowaniu procesowym*, „Monitor Prawniczy" Nr 4/1997; J. Jankowski: *Problemy nowelizacji KPC – postępowanie rozpoznawcze*, „Monitor Prawniczy" z 16 maja 2005 r. (sprawozdanie z seminarium), http://www.monitorprawniczy.pl/index.php?mod=m_aktualnosci&cid=21&id=877.

[401] Ściśle rzecz ujmując, nie ma i nie może być dwóch różnych prawd odnośnie do tego samego stanu (wg klasycznej – arystotelesowskiej – definicji bowiem prawdziwe jest zdanie, którego treść jest zgodna z rzeczywistością), stąd też o „prawdzie formalnej" można mówić jedynie w sensie przenośnym, dlatego też w niniejszej monografii jest ona pisana w cudzysłowie.

co nie jest prawdziwe. Rolą biegłego jest bowiem służyć sądowi swoimi wiadomościami specjalnymi z dziedziny, dla której został ustanowiony, a nie wprowadzać go w błąd, nawet jeśli czynią to zgodnie znajdujące się w sporze strony. Jeśli więc strony sporu cywilnego będą zgodnie twierdzić, że prawdą jest zdanie fałszywe (o czym biegły wie z uwagi posiadania wiadomości specjalnych), to biegły nie może oprzeć na takiej fałszywej przesłance swojej opinii[402]. Natomiast z zasady kontradyktoryjności wynika tyle tylko, że biegły nie może sugerować uzupełnienia materiału dowodowego czy przeprowadzenia dodatkowych badań. Mogłoby to bowiem być odebrane jako doradzanie stronom w zakresie taktyki postępowania przed sądem i skutkować wysoce nieprzyjemnymi dla biegłego konsekwencjami. Oczywiście zadaniem biegłego w ogóle (czy to w procesie cywilnym czy też karnym), nie jest udzielanie porad stronom, a do jego kompetencji nie należy wykraczanie poza zakres opinii, natomiast w procesie karnym stosunkowo często zdarza się i jest w pełni uprawnioną sytuacja, w której biegły sugeruje sposób dotarcia do prawdy (materialnej), bowiem – co oczywiste – strony ani sąd mogą nie znać takiego sposobu (np. metodologii badań danej dyscypliny czy aktualnego stanu techniki), o ile należy on do dziedziny wiadomości specjalnych. Dotarcie do prawdy (materialnej) jest nadrzędną zasadą zarówno sądu karnego, jak i organu prowadzącego postępowanie przygotowawcze. W procesie cywilnym natomiast biegły nie wie, czy taktyką stron nie jest oparcie się na „prawdzie" formalnej, nieko-

[402] W jednym z postępowań, w którym autor miał okazję występować w roli biegłego, spór dotyczył domniemanej niezgodności zarządzania projektem informatycznym przez zewnętrzną, wynajętą do tego celu firmę, z jedną z metodyk zarządzania projektami. Strona powodowa (organizacja, na rzecz której realizowano przedsięwzięcie) uważała, że pozwana firma (firma zarządzająca projektem i realizująca go) prowadząc projekt wg tej metodyki, naruszała w kilku miejscach zalecenia metodyki, strona pozwana – że do takiego naruszenia nie doszło. Pytania zadane biegłemu dotyczyły zgodności pewnych detali tejże metodyki i sposobu ich realizacji w spornym projekcie, zaś problem leżał w tym, że metodyka, o której mówiły strony nie była w ogóle metodyką zarządzania projektami, choć obie strony sądziły akurat inaczej. W takiej sytuacji, oczywiście biegły nie może przyjąć „prawdy" formalnej stojącej w sprzeczności z wiedzą biegłego i stanem faktycznym i na niej budować swoich rozważań, musi natomiast poinformować organ procesowy o zaistniałej sytuacji.

niecznie odpowiadającej prawdzie (materialnej), albo, czy któraś ze stron nie jest zdecydowana – nawet za cenę ewentualnej przegranej w sporze sądowym – nie ujawniać publicznie jakichś faktów i okoliczności[403]. Jedna i druga sytuacja może mieć miejsce i – w świetle obowiązujących przepisów – taka postawa stron jest w pełni dopuszczalna, więc biegły musi działać w ten sposób, aby takiej ewentualnej taktyki nie zniweczyć[404]. Jak się wydaje, zakaz wnioskowania o uzupełnienie materiału dowodowego nie dotyczy sytuacji ewidentnych: można zaryzykować twierdzenie, że nie popełnia błędu biegły, który – poruszając się w ramach zakreślonego przez sąd zakresu opinii – zwróci się do sądu z informacją o konieczności „technicznego" uzupełnienia materiału dowodowego[405]. Na marginesie warto poruszyć też kwestię korzystania przez biegłego z informacji niedostarczonej przez stronę, ale będącej informacją publiczną, wobec której nie dokonano ograniczenia jawności[406]: można, jak się wydaje, spodziewać się, że skorzystanie z informacji publicznej nie jest nieuprawnionym samodzielnym rozszerzeniem przez biegłego materiału dowodowego, analogicznie trudno byłoby za takowe uznać skorzystanie z informacji zawartej w pod-

[403] Klasycznym przykładem takiego konsensusu, prowadzącego do wytworzenia „prawdy" formalnej, może być np. zgodne wnioskowanie małżonków o udzielenie rozwodu bez orzekania o winie (nawet jeśli jedna ze stron ponosi zań rzeczywistą winę) motywowane chęcią nieupubliczniania szczegółów ich pożycia małżeńskiego.

[404] W cytowanym artykule (P. Kowalski, J. Składzień: *Opiniowanie*…, op. cit.) opisano jako przykład działanie biegłego, który – bez związku z zakresem opinii – z własnej inicjatywy poinformował w opinii sąd i strony, jakie badania lekarskie należy wykonać dla udowodnienia twierdzeń jednej ze stron.

[405] Z własnej praktyki autora można podać przypadek, w którym biegły miał wypowiedzieć się na temat programu komputerowego, którego kod źródłowy ani program wynikowy nie były umieszczone w przedstawionym materiale. Oczywiście formalnie możliwe było zapewne wydanie opinii nierozstrzygającej z powodu braku przedmiotu badania natomiast rozsądniejszym z punktu widzenia ekonomii postępowania było zwrócenie się do sądu o uzupełnienie materiału dowodowego poprzez zwrócenie się do stron o dostarczenie tegoż przedmiotu badania. Trudno uznać taki wniosek za sugerowanie stronie taktyki dowodzenia swoich racji.

[406] Z tego rodzaju sytuacją można spotkać się przy opiniowaniu przy okazji sporów przed Krajową Izbą Odwoławczą (z formalnego punktu widzenia jest to postępowanie przed sądem polubownym, a więc postępowanie cywilne). Często strony nie dostarczają pełnej dokumentacji postępowania o udzielenie zamówienia publicznego, jest ona natomiast dostępna np. w Biuletynie Informacji Publicznej.

ręczniku czy encyklopedii, nawet jeśliby biegły czerpał z niej informacje nie tylko metodologiczne, ale i o stanach rzeczowych.

Można mieć szereg wątpliwości – zarówno natury moralnej, jak i technicznej – co do usunięcia w 1996 r. regulacji z art. 3 § 2 KPC tego przepisu, który dawał podstawę do skonstruowania zasady prawdy obiektywnej (prawdy materialnej). W praktyce biegłego informatyka nie powoduje ono raczej wspomnianego wcześniej „przyspieszenia i uproszczenia postępowania", a wręcz przeciwnie – strony stosunkowo często dostarczają niekompletną dokumentację techniczną czy projektową, zaś dopiero wydawane na jej podstawie opinie (kończące się często konkluzją „na podstawie przedstawionego materiału nie można wyciągnąć kategorycznych wniosków") skłaniają je do uzupełnienia materiału dowodowego i wnioskowania o kolejne opinie, przy czym taka sytuacja potrafi powtarzać się wielokrotnie. Strony bowiem (i ich pełnomocnicy procesowi) często nie są przekonane o potrzebie skorzystania z pomocy „prywatnych" ekspertów i ustalają taktykę swojego postępowania niejako metodą prób i błędów, ponieważ biegły w postępowaniu cywilnym nie może im – zgodnie z tym, co napisano powyżej – w tym w żaden sposób pomóc. Biegłemu pozostaje cierpliwie znosić taką metodę pracy i liczyć na domyślność stron albo na decyzję sądu, który zdecyduje się jednak pokierować się zasadą prawdy (materialnej) i zapyta biegłego o sugerowany sposób dotarcia do niej. Pytania „co należy uczynić, aby udowodnić, że …"[407] czy „jakie dokumenty powinienem przedstawić" zdarzają się w sprawach informatycznych stosunkowo często. Jeśli pytanie takie zadaje strona, zdaniem autora, biegły może i powinien zwrócić się do sądu z pytaniem, czy ma na tak postawione pytanie odpowiedzieć, biorąc pod uwagę, że może ono zasugerować stronom sposób postępowania i – w przypadku otrzymania odpowiedzi pozytywnej – udzielić nań odpowiedzi. Oczywiście również na takie pytanie zadane przez sąd należy udzielić odpowiedzi. Ewentualna odpowiedzialność w takim wypadku spada bowiem nie na biegłego, a na organ procesowy, którego jest narzędziem.

[407] Por. P. Kowalski, J. Składzień: *Opiniowanie*…, op. cit.

Zakończenie

Rozwój tzw. wysokich technologii (a więc między innymi informatyki i telekomunikacji), powoduje rosnącą złożoność rozwiązań, które stają się immanentną częścią życia społecznego. Co za tym idzie, do sądów coraz częściej trafiają sprawy, w których istotą sporu jest inne niż oczekiwane działanie systemu informatycznego, skutki ujawnionych w nim błędów czy celowe naruszanie jego bezpieczeństwa. Nawet w sprawach „tradycyjnych" standardowo już wśród zabezpieczanych dowodów rzeczowych znajdują się urządzenia i dane teleinformatyczne: telefony komórkowe, komputery osobiste, systemy nawigacji GPS, nośniki cyfrowe, dane bilingowe telefonów komórkowych itp. Wraz z rozwojem i upowszechnieniem technik informatycznych rośnie rola ekspertów, a w szczególności biegłych występujących w postępowaniach przed organami wymiaru sprawiedliwości, organami ścigania i organami administracji publicznej.

W ramach niniejszej monografii podjęto próbę usystematyzowania zagadnień związanych z naukowym aspektem opiniowania sądowo-informatycznego, w szczególności proponując rozpatrywanie go dwojako:

- w obrębie informatyki (informatyki stosowanej), jako informatykę sądową będącą odpowiednikiem tradycyjnych „dyscyplin pomostowych" takich jak medycyna sądowa czy psychiatria sądowa;
- w obrębie technik kryminalistycznych w odniesieniu do poszczególnych metod „informatyki śledczej".

Przynajmniej część zagadnień związanych z opiniowaniem (opiniowanie w sprawach karnych, kryminalistyka komputerowa) z natury rzeczy musi znajdować się również w obrębie zainteresowań nauk policyjnych (które w Polsce nie są formalnie wyodrębnione w istniejących przepisach), a więc w ramach nauk o bezpieczeństwie.

Dokonano próby systematyzacji i przeglądu najważniejszych ról opiniodawczych, jakie może pełnić informatyk: roli doradcy, eksperta, audytora oraz biegłego. W odniesieniu do tej ostatniej zebrano i przeanalizowano najważniejsze uwarunkowania metodologiczne w odniesieniu do postępowań cywilnych i najczęściej spotykanych rodzajach spraw karnych. Osobno zebrano uwagi dotyczące opiniowania w sprawach związanych z tzw. przestępstwami komputerowymi, które są dla informatyków sądowych ważne nie tylko jako poszczególne studia przypadków, ale przede wszystkim jako źródło wiedzy na temat tego, jak w praktyce orzeczniczej traktuje się poszczególne techniki i narzędzia informatyczne, a nawet jak rozumiane są podstawowe pojęcia (takie jak „informacja", „dane" czy „sieć").

Polski system prawny pozostawia wiele do życzenia, jeśli idzie o klarowność przepisów dotyczących biegłych. W systemach informacji prawniczej wyszukiwanie aktów prawnych zawierających słowo „biegły" wskazuje na ponad sto różnych ustaw i rozporządzeń. Postulat regulacji statusu biegłych jednym aktem rangi ustawowej podejmowany jest przez kolejnych ministrów sprawiedliwości i kolejne rządy (a nawet raz jako poselska inicjatywa ustawodawcza), niestety jak dotychczas bezskutecznie. Kolejne projekty ustaw wahają się pomiędzy skrajnościami: od wersji w zasadzie tylko powtarzającej rozwiązania istniejące w kolejnych rozporządzeniach Ministerstwa Sprawiedliwości (jak również dawnego Ministerstwa Spraw Wewnętrznych i Administracji), po projekty rewolucyjne, odbierające zagadnienia biegłych władzy sądowniczej i powierzające nadzór nad nimi władzy wykonawczej. Nie można jednak nie odnieść wrażenia, że w przytłaczającej większości wariantów tych projektów najważniejszym zagadnieniem jest pogodzenie interesów władzy sądowniczej i władzy wykonawczej, zaś interesy i postulaty samych biegłych nie przedstawiają dla projektodawców jakiejś szczególnej wartości. Dopóki ten stan rzeczy nie ulegnie zmianie, dopóty można obawiać się, że liczba krytycznych (a często uzasadnionych) uwag o jakości pracy biegłych nie zmaleje.

Kolejną kwestią, z którą przyjdzie się zmierzyć biegłym (choć przede wszystkim sędziom i prokuratorom) są uchwalone już zmiany w procedurze karnej, które mają wejść w życie w lipcu 2015 roku, a co do których już teraz zgłaszane są liczne zastrzeżenia i postulaty nowelizacji. Nieostrożne

zwiększenie znaczenia zasady kontradyktoryjności w postępowaniu karnym może prowadzić – w zakresie interesującym z punktu widzenia niniejszej monografii – do szeregu niekorzystnych zjawisk, wśród których można wymienić choćby zagrożenie nieetycznymi zachowaniami ze strony specjalistów powoływanych na wniosek stron (takie zjawisko występuje, ale póki co, w przypadku opiniowania informatycznego jest raczej marginalne), czy trudnościami z przeprowadzeniem badań dla stron postępowania, jeśli materiał dowodowy znajduje się w gestii drugiej strony (podobne problemy pojawiają się w procedurze cywilnej). Wpływ zmian na uwarunkowania metodologiczne procesu opiniowania, jest o tyle na razie trudny do przewidzenia, że będzie determinowany również przez praktykę orzeczniczą, która będzie musiała się dopiero ukształtować. Można być jednak przekonanym, że – zarówno z uwagi na rozwój samych „wysokich technologii", jak i na zmiany zachodzące w systemie prawnym – zagadnienia opiniowania sądowo-informatycznego pozostaną jeszcze przez długi czas zagadnieniami ważkimi ze społecznego i ekonomicznego punktu widzenia i interesującymi z punktu widzenia nauki i praktyki.

Załącznik. Dobre praktyki – badanie dysku twardego

(Dokument opracowany przez Sekcję Informatyki Sądowej Polskiego Towarzystwa Informatycznego, rekomendowany przez Pracownię Badań Komputerów Laboratorium Kryminalistycznego Komendy Wojewódzkiej Policji w Łodzi, wersja 0.3. z 14 grudnia 2009 r.)

Rozpoczęcie badań.

1. Podczas pracy z dyskiem używaj zabezpieczeń przed elektrycznością statyczną (mata uziemiająca, opaski na ręce).

2. Wykonaj dokumentację fotograficzną oraz opisową zapewniającą jednoznaczną identyfikację dostarczonego do badań materiału dowodowego. Uwzględnij widoczne uszkodzenia dysku: wgniecenia, otwory itd. Jeśli stan uszkodzeń wskazuje na to, że uruchomienie dysku mogłoby doprowadzić do jego zniszczenia rozważ wymianę obudowy i elektroniki dysku.

3. Podłącz dysk za pośrednictwem urządzeń sprzętowych uniemożliwiających modyfikację analizowanych danych tzw. *write-blockerów*.

4. Wykonaj kopię bitową dysku[A] na inny nośnik, a następnie kopię tejże kopii. Podczas wykonywania kopii oblicz sumę kontrolą SHA1 lub/i MD5. Jeśli to konieczne wykonaj w analogiczny sposób kopie partycji i dysków logicznych.

[A] Komentarz: należy wykonać przede wszystkim kopię bitową dysku (całego nośnika), a nie pojedynczych partycji czy dysków logicznych (te mogą być wykonane w dalszej kolejności). Kopie partycji i dysków logicznych należy wykonać bez montowania systemów plików znajdujących się na dyskach logicznych (w tablicach opisujących alokację plików i katalogów na dyskach mogą być fałszywe informacje o zawartości poszczególnych klastrów np. fałszywe *bad sectory*, w których ukrywają się kody wirusów itd.).

5. Opisz dokładnie narzędzie, za pomocą którego wykonałeś kopię bitową (nazwa, wersja) oraz sposób w jaki narzędzie traktuje bloki nie dające się odczytać[B].

6. Wszystkie dalsze prace wykonuj na kopiach bitowych.

7. Przeprowadź badania komputerowe:

✓ opisz narzędzia, w tym oprogramowanie oraz przyjętą metodologie badań, zastosowaną w opracowaniu opinii;

✓ sporządź listę partycji, dysków logicznych na partycjach (wraz z systemami plików zainstalowanymi na tych dyskach) oraz listę plików wraz z czasami MAC oraz sumami kontrolnymi SHA1 lub/i MD5 każdego pliku[C];

✓ sprawdź kopie bitowe (tj. znajdujące się na nich pliki, obrazy *bootsectorów*, tablice alokacji plików itd.) na obecność wirusów i koni trojańskich;

✓ przeprowadź badania zgodnie z postawionymi przez zleceniodawcę pytaniami.

Zakończenie badań.

1. Formułuj czytelne oraz logiczne wnioski używając słownictwa zrozumiałego dla odbiorcy niemającego wykształcenia informatycznego.

Jeśli na dysku twardym zostanie ujawnione oprogramowanie mogące mieć wpływ na działanie systemu informatycznego (np. wirusy, robaki, konie trojańskie) opisz je w opinii[D].

[B] Komentarz: różne narzędzia do wykonywania kopii bitowych mogą różnie traktować błędy odczytu (np. wypełnianie różnymi wzorcami, pomijanie bloków) co może powodować niezgodności sum kontrolnych przy ewentualnej późniejszej weryfikacji wierności kopii.

[C] Komentarz: większość badań dotyczy zawartości plików nie zaś niezaalokowanych obszarów dysku. Na dyskach, w szczególności przechowywanych w nieodpowiednich warunkach przez dłuższy czas, mogą pojawić się uszkodzone sektory. W przypadku, w którym policzono jedynie sumę kontrolą całego dysku, jeśli w trakcie późniejszego postępowania pojawi się konieczność zweryfikowania wierności kopii, znajomość sum kontrolnych poszczególnych plików może pozwolić na znalezienie miejsca powstania błędu lub kontynuowanie pracy mimo częściowego uszkodzenia śladów.

[D] Komentarz: obecność trojanów może świadczyć o tym, że komputer użyty był jako zombie, a w szczególności że wykonywał operacje bez wiedzy swojego posiadacza.

3. W opinii określ stanowczość wniosków[E] i wiarygodność metod, z których korzystałeś[F].

4. Wykonaj na nośnik jednokrotnego zapisu kopie plików, uwzględnionych w opinii, policz sumy kontrolne SHA1 lub/i MD5 plików na tym nośniku i samego nośnika i zapisz je w opinii (w części napisanej na papierze).

5. Na wyraźne życzenie zlecającego dołącz do opinii kopię bitową badanego nośnika na nośnikach optycznych jednokrotnego zapisu (np. dysk DVD, Blue Ray).

6. Zabezpiecz urządzenia w opakowania zapewniające nienaruszalność oraz integralność materiału dowodowego. Opakowania winny stanowić izolację przed wilgocią, temperaturą, elektrycznością statyczną, wstrząsami itp.

7. Dołącz informacje o materiale dowodowym[G].

8. Po dostarczeniu opinii i dowodów do zlecającego i pokwitowaniu przez niego ich otrzymania zniszcz wszelkie kopie badanego dysku i plików na nim się znajdujących w sposób uniemożliwiający ich odtworzenie. O fakcie zniszczenia kopii materiałów dowodowych powiadom zlecającego np. w opinii lub oddzielnym pismem.

[E] Komentarz: można używać np. skali stopniowania kategoryczności wniosków zaproponowanej w pracy J. Wójcikiewicza: *Ekspertyza sądowa*, pod red. J. Wójcikiewicza, Zakamycze, Kraków 2002:

- ✓ pozytywne wnioski stanowcze, zwane też kategorycznymi;
- ✓ pozytywne wnioski uprawdopodabniające;
- ✓ pozytywne wnioski niewykluczające;
- ✓ wnioski nierozstrzygające;
- ✓ uprawdopodabniające wnioski negatywne;
- ✓ niewykluczające wnioski negatywne;
- ✓ stanowcze wnioski negatywne.

[F] Komentarz: zapisy informacji na dyskach mogą być sfałszowane bądź nie odpowiadać rzeczywistości (np. stosunkowo łatwo sfałszować metadane dotyczące czasów MAC, pracując w komputerze ze źle ustawionym zegarem), niektóre z informacji znalezionych na dysku mogą być potwierdzone przez wykorzystanie źródeł zewnętrznych (np. fakt zalogowania się w określonym czasie na serwer może być odnotowany w logach tegoż serwera) co może pozwolić organowi zlecającemu opinię na uzyskanie stanowczych wniosków.

[G] Komentarz: w celu późniejszej identyfikacji materiału dowodowego przez zleceniodawcę powinny być umieszczone takie dane jak: „nazwa zleceniodawcy, numer sprawy (nadany przez zleceniodawcę), cechy jednoznacznie identyfikujące materiał dowodowy (np. numer seryjny, naniesione oznaczenie)".

Bibliografia

[1] *15-latka ukradła ekwipunek wirtualnemu wojownikowi*, http://www.policja.pl/pol/aktualnosci/84554,dok.html

[2] *17-latkowi grozi poprawczak za wirtualną kradzież*, http://www.dziennik lodzki.pl/artykul/425623,17latkowi-grozi-poprawczak-za-wirtualna-kradziez,id,t.html

[3] A. Adamski: *Cyberprzestępczość – aspekty prawne i kryminologiczne*, „Studia Prawnicze" Nr 4/2005

[4] A. Adamski: *Opinia do projektu ustawy z druku nr 458 Rządowy projekt ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw*, Biuro Analiz Sejmowych, Toruń 4 lipca 2008 r., http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf

[5] A. Adamski: *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000

[6] J. Apanowicz: *Metodologiczne elementy procesu poznania naukowego w teorii organizacji i zarządzania*, WSAiB, Gdynia 2000

[7] J.J. Barbara: *Triage A Computer*, "Forensic Magazine", http://www.forensicmag.com/articles/2010/06/triage-computer#.Ur34p42x9i4

[8] J. Barta, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski: *Prawo autorskie i prawa pokrewne. Komentarz*, Wolters Kluwer, Warszawa 2011

[9] J. Barta [w:] *System prawa prywatnego. Prawo autorskie*. Tom 13, pod red. Z. Radwańskiego, Warszawa 2007

[10] B. Batóg, K. Wawrzyniak: *Diagnozowanie A Prognozowanie Ekonometryczne – Podobieństwa, Różnice, Zależności*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego" Nr 394, „Prace Katedry Ekonometrii i Statystyki" Nr 15/2004, Szczecin 2004, s. 21–33

[11] A. Baworowski: *Problemy wykładni przepisów art. 268 § 2, 269 § 2 i 269a KK po nowelizacjach z 2008 r.*, „Diariusz Prawniczy" Nr 10/11/2009

[12] J.M. Bocheński: *Współczesne metody myślenia*, W drodze, Poznań 1988
[13] J. Bocheński: *Autonomia Uniwersytetu* [w:] *Sens życia i inne eseje*, PHILED, Kraków 1993, s. 60–72
[14] J. Bocheński: *Sto zabobonów. Krótki filozoficzny słownik zabobonów*, PHILED, Kraków 1994
[15] J. Bocheński: *Wspomnienia*, PHILED, Kraków 1994
[16] A. Bojańczyk: *Karnoprawne aspekty ochrony prawa pracownika do tajemnicy komunikowania się (Część II)*, „Palestra" Nr 3/2003, http://www.palestra.pl/index.php?go=artykul&id=941
[17] M. Bojarski: *Problemy odpowiedzialności karnej i dyscyplinarnej biegłego*, „Jurisprudencija" 2000, t. 18(10), s. 24–28
[18] G. Borkowski: *VAT od sprzedaży programów komputerowych*, „Glossa" Nr 3/2004, http://www.czasopisma.pwp.pl/glosa-200403.xml?katalog=2004038
[19] S. Bukowski: *Projekt zmian Kodeksu karnego – Dostosowanie do Konwencji o cyberprzestępczości*, „Gazeta Sądowa" kwiecień 2004, http://www.prawo.lex.pl/czasopisma/gs/pzmiankk.html
[20] Ľ. Čech: *Bezpečnostné aspekty vzdelávania profesionálov ozbrojených síl SR – pohľad učiteľa spoločenských vied* [w:] *Bezpečnosť a bezpečnostná veda, Liptovský Mikuláš*, Akadémia ozbrojených síl generála M.R. Štefánika, 2009, s. 219–224
[21] K. Cetnarowicz, R. Cięciwa, E. Nawarecki, G. Rojek*: Unfavorable Behavior Detection in Real World Systems Using the Multiagent System*, Intelligent Information Systems and Web Mining: proceedings of the international IIS: IIPWM '05 conference: Gdansk, Poland, June 13–16, 2005, s. 416–420
[22] P. Chlebowicz: *Perspektywy wykorzystania analizy kryminalnej w praktyce prokuratorskiej*, „Prokuratura i Prawo" Nr 7–8/2013, s. 263–277
[23] J. Curyło: *Przestępstwa przeciwko mieniu (art. 278art. 294 KK)*, Szkoła Policji w Pile, Piła 2011, http://isp.policja.pl/download/12/1537/przeciwkomieniu.pdf
[24] J. Dworzecki: *Terroryzm jako zagrożenie współczesnego świata*, Zeszyt Naukowy „Apeiron" Nr 5, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego w Krakowie, Kraków 2011, s. 181–232

[25] T. Dyrda: *Informatyka śledcza, V Międzynarodowy kongres audytu, kontroli wewnętrznej oraz procedur zwalczania oszustw i korupcji*, Kraków 2006, maszynopis, http://webapp01.ey.com.pl/EYP/WEB/eycom_download.nsf/resources/Informatyka_sledcza_TD_pl.pdf/$FILE/Informatyka_sledcza_TD_pl.pdf
[26] K. Eichstaedt, P. Gałecki, A. Depko: *Metodyka pracy biegłego psychiatry, psychologa oraz seksuologa w sprawach karnych*, LexisNexis, Warszawa 2012
[27] B. Fischer: *Przestępstwa komputerowe i ochrona informacji*, Zakamycze, Kraków 2000
[28] M. Forystek: *Audyt informatyczny*, InfoAudit, Warszawa 2005
[29] P. Frankowski: *Komputerowi detektywi. 111 porad*, Mikom, Warszawa 2005
[30] M. Frydrych, I. Kondracka: *Pomógł policji – stracił komputer*, http://fakty.interia.pl/news/pomogl-policji-stracil-komputer,1439333/600bd8ff8c340a70559ecec3f70b676f
[31] A. Gaberle: *Dowody w sądowym procesie karnym*, Wolters Kluwer, Warszawa 2007
[32] *Prokuratura powołuje jasnowidza Jackowskiego jako biegłego. Pierwszy taki przypadek w Polsce?*, http://wiadomosci.gazeta.pl/wiadomosci/1,114871,14000927,Prokuratura_powoluje_jasnowidza_Jackowskiego_jako.html
[33] K. Gienias: *Dystrybucja kopii utworów za pomocą aplikacji peer to peer (P2P)*, „Prokurator" Nr 4/2005 s. 72–79, http://www.sprp.com.pl/tresc/prokurator/6da368d4e4c3ed60007775cf200ace37.pdf
[34] K. Gienias: *Eliminacja „Rajów Hackerskich" czy ograniczenie metod badania systemów informatycznych* [w] J. Kosiński: *Przestępczość teleinformatyczna, IX seminarium naukowe*, pod. red J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2006, s. 31–38
[35] K. Gienias: *Odpowiedzialność prawna a ochrona sieci WLAN*, „Computerworld" z 9 lutego 2009 r., http://www.computerworld.pl/artykuly/336381/Odpowiedzialnosc.prawna.aochrona.sieci.WLAN.html
[36] R. Golat: *Prawo autorskie i prawa pokrewne*, C.H. Beck, Warszawa 2006
[37] J. Gościński: *Zarys sterowania ekonomicznego*, PWN, Warszawa 1977

[38] B. Grabowska, A. Pietryka, M. Wolny, A. Bodnar: *Raport HFPC: Biegli sądowi w Polsce*, http://www.hfhr.pl/wp-content/uploads/2014/04/HFPC_PRB_biegli-sa%CC%A8dowi_w_polsce.pdf

[39] A. Gruszka: *ISO 19011:2011 Wytyczne auditowania systemów zarządzania – najważniejsze zmiany*, „Wiadomości PKN" Nr 1/2013, s. 8–11, http://www.pkn.pl/sites/default/files/w1_2013.pdf

[40] E. Gruza, M. Goc, J. Moszczyński: *Kryminalistyka – czyli rzecz o metodach śledczych*, WAiP, Warszawa 2008

[41] E. Gruza: *Ocena wiarygodności zeznań świadków w procesie karnym. Problematyka kryminalistyczna*, Zakamycze, Kraków 2003

[42] T. Grzegorczyk: *Kodeks Postępowania Karnego oraz ustawa o świadku koronnym*, pod red. T. Grzegorczyka, Wolters Kluwer, Warszawa, 2008

[43] A. Grześkowiak, K. Wiak: *Kodeks karny. Komentarz*, pod red. A. Grześkowiak, K. Wiaka, C.H. Beck, Warszawa 2012

[44] K. Grzybczyk, A. Auleytner, K. Kulesza: *Prawo w wirtualnych światach*, pod red. K. Grzybczyk, Difin, Warszawa 2013

[45] J. Gurgul: *O swobodnej ocenie opinii biegłego*, „Prokuratura i Prawo" Nr 10/2013, s. 34–56, http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2013/10/3gurgul.pdf

[46] T. Hanausek: *Kryminalistyka – zarys wykładu*, Zakamycze, Kraków 2005

[47] S. Hoc: *Karnoprawna ochrona informacji*, Uniwersytet Opolski, Opole 2009

[48] P. Hofmański, S. Zabłocki: *Elementy metodyki pracy sędziego w sprawach karnych*, Wolters Kluwer, Warszawa, 2011

[49] L. Hofreiter: *Wstęp do studiów bezpieczeństwa*, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Kraków 2012

[50] L. Hofreiter: *Securitológia. Liptovský Mikuláš*, Akadémia ozbrojených síl gen. M.R. Štefánika, 2006

[51] L. Hofreiter: *Teória a riešenie konfliktov. Liptovský Mikuláš, Akadémia ozbrojených síl gen M.R. Štefánika*, 2008

[52] L. Hofreiter, et.al: *Determinovanosť vojenských plánovacích a rozhodovacích procesov podmienkami informačného zabezpečenia*, VA , Liptovský Mikuláš, 2003

[53] *IDC Whitepaper: The Diverse and Exploding Digital Universe. An Updated Forecast of Worldwide Information Growth Through 2011*, http://www.ifap.ru/library/book268.pdf
[54] K. Jaegermann: *Opiniowanie sądowo-lekarskie. (Eseje o teorii)*, Wydawnictwo prawnicze, Warszawa 1991
[55] K.J. Jakubski: *Przestępczość komputerowa – zarys problematyki*, „Prokuratura i Prawo" Nr 12/1996
[56] P. Janas: *Przestępstwo hackingu*, „Prokuratura i Prawo" Nr 10/2009, s. 27–34
[57] J. Jankowski: *Problemy nowelizacji KPC – postępowanie rozpoznawcze*, „Monitor Prawniczy" z 16 maja 2005 r. (sprawozdanie z seminarium) http://www.monitorprawniczy.pl/index.php?mod=m_aktualnosci&cid=21&id=877
[58] H.G. Jaschke: *Policyjna nauka – podejście europejskie*, CEPOL 2008, https://www.cepol.europa.eu/fileadmin/website/Research_Science/PGEAPS/PGEAPS_summary_polish.pdf
[59] J. Jerzewska: *Od oględzin do opinii biegłego. Poradnik dla prowadzących postępowanie karne*, Dom Wydawniczy ABC, Warszawa 2005
[60] A. Kallaus: *Konsekwencje prawne zmiany przepisu art. 3 KPC w postępowaniu procesowym*, „Monitor Prawniczy" Nr 4/1997
[61] M. Karolewski: *Przestępstwa przeciwko ochronie informacji w Kodeksie Karnym z 1997 roku ze szczególnym uwzględnieniem art. 267 § 1 jako przepisu kryminalizującego „hacking" na tle unormowań Rady Europy*, praca magisterska napisana w Zakładzie Prawa Karnego Porównawczego pod kierunkiem Anny Walczak Żochowskiej, Warszawa 2005, http://prawo.vagla.pl/files/mgr_m_karolewski.pdf
[62] S. Koc: *Karnoprawna ochrona informacji*, Wydawnictwo Uniwersytetu Opolskiego, Opole 2009
[63] A. Kegel, Z. Kegel: *Przepisy o biegłych sądowych, tłumaczach i specjalistach. Komentarz*, Zakamycze, Kraków 2004
[64] A. Kiedrowicz-Wywiał: *Pharming i jego penalizacja*, „Prokuratura i Prawo" Nr 6/2011, s. 24–36
[65] Ł. Kister: *Bezpieczeństwo informacyjne infrastruktury krytycznej*, „Terroryzm" Nr 1/2010, Collegium Civitas, Warszawa 2010, s. 6–9

[66] L. Klander: *Hacker proof, czyli jak się bronić przed intruzami*, Mikom, Warszawa 1997

[67] L. Klander: *Hacker Proof: The Ultimate Guide to Network Security*, Jamsa Pr., 1997

[68] M. Kliś, T. Martiszek: *Przestępstwa elektroniczne*, http://prawo.vagla.pl/skrypts/cybercrime1.htm

[69] M. Kliś: *Przestępczość w Internecie*, „Czasopismo prawa karnego i nauk penalnych" Nr 1/2000

[70] M. Kobylas: *Analiza kryminalna w Polsce. Ewolucja w kierunku GIS*, http://www.konferencja.esri.pl/sites/default/files/M.Kobylas_WSP%20w%20Szczytnie.pdf

[71] *Kodeks etyki pracownika naukowego przyjęty 13 grudnia 2012 r. przez Zgromadzenie Ogólne PAN*, http://www.instytucja.pan.pl/images/stories/pliki/Komisja_ds_Etyki_Nauce/dokumenty/Kodeks_etyki_pracownika_naukowego_31.12._2012.pdf

[72] P. Konieczny: *„Głębokie ukrycie" danych w PKO BP*, http://niebezpiecznik.pl/post/glebokie-ukrycie-danych-w-pko-bp/

[73] G. Kopczynski: *Konfrontacja biegłych w polskim procesie karnym*, Wolters Kluwer business, Warszawa 2008

[74] L. Kordylewski: *Forensyka, Forensic Science Center*, http://www.kordy net.com/forensyka.html.

[75] L.F. Korzeniowski: *Firma w warunkach ryzyka gospodarczego*, EAS, Kraków 2002

[76] L.F. Korzeniowski: *Nauki o bezpieczeństwie – wprowadzenie do problematyki* [w:] P. Cybula: *Prawne aspekty bezpieczeństwa w górach: turystyka, rekreacja, sport*, pod red. P. Cybuli, COTG PTTK, Kraków 2013, s. 257–272

[77] L.F. Korzeniowski: *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa 2012

[78] J. Kosiński: *Przestępczość teleinformatyczna IX seminarium naukowe*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2006

[79] J. Kosiński: *Przestępczość teleinformatyczna VII seminarium naukowe*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2004

[80] J. Kosiński: *Przestępczość teleinformatyczna VIII seminarium naukowe*, pod red. J. Kosińskiego,Wyższa Szkoła Policji, Szczytno 2005

[81] J. Kosiński: *Przestępczość teleinformatyczna X seminarium naukowe*, pod red. J. Kosińskiego,Wyższa Szkoła Policji, Szczytno 2007
[82] J. Kosiński: *Przestępczość teleinformatyczna XII seminarium naukowe*, pod red. J. Kosińskiego,Wyższa Szkoła Policji, Szczytno 2009
[83] J. Kosiński, J. Szafrański: *Przestępczość teleinformatyczna XI seminarium naukowe*, pod red. J. Kosińskiego, J. Szafrańskiego, Wyższa Szkoła Policji, Szczytno 2008
[84] T. Kotarbiński: *Elementy teorii poznania, logiki formalnej i metodologii nauk*, Warszawa, PWN 1986
[85] P. Kowalski, J. Długopolski: *Kategoryczność opinii biegłego sądowego medyka w sprawach cywilnych*, „Palestra" Nr 9–10/2008, http://www.palestra.pl/index.php?go=artykul&id=2808
[86] P. Kowalski, J. Składzień: *Opiniowanie w sprawach cywilnych i karnych jako problem w praktyce biegłego*, „Otorynolaryngologia" Nr 3(3)/2004
[87] S. Kozdrowski: *Kryminalistyka. Wybrane zagadnienia*, NWSP, Białystok 2012
[88] R. Krajewski: *Przestępstwo utrwalania i rozpowszechniania wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej*, „Prokuratura i Prawo" Nr 5/2012 s. 20–40
[89] M.P. Krysiak: *Biegły (pytania do biegłych)*, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2005
[90] *Kto zabrał broń za 900 zł postaci z gry internetowej*, http://olsztyn.gazeta.pl/olsztyn/1,35189,8181779,Kto_zabral_bron_za_900_zl_postaci_z_gry_internetowej.html
[91] B.R. Kuc: *Funkcje nauki. Wstęp do metodologii. Nauka nie jest grą*, Wydawnictwo PTM, Warszawa 2012
[92] M. Kuczyńska-Cichocka: *Biegły, ale czy na pewno specjalista*, „Profesjonalny parkiet" Nr 3/2008, http://terazmedia.nazwa.pl/pparkiet/index.php?option=com_content&task=view&id=36
[93] J.P. Kufel: *Taktyka przesłuchania świadka*, „Edukacja Prawnicza" z 13 października 2009 r., http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualnosc/art/taktyka-przesluchania-swiadka.html
[94] J. Kulesza, J. Kulesza: *Gra „Second Life" – wirtualny świat, realne przestępstwa?*, „Prokuratura i Prawo" Nr 3/2009, s. 23–40

[95] B. Kunicka-Michalska: *Komentarz do artykułów 222-316* [w:] A. Wąsek, R. Zawłocki: *Kodeks Karny. Część szczegółowa*, C.H. Beck, Warszawa 2010

[96] J. Kunz: *Błąd w opiniach sądowo-lekarskich w sprawach przestępstw przeciwko zdrowiu i życiu*, Katedra Medycyny Sądowej Collegium Medicum UJ, Kraków 1999

[97] V. Kwiatkowska-Wójcikiewicz: *Glosa do wyroku Sądu Najwyższego z dnia 3 października 2006 r., sygn. IV KK 209/06*, „Prokuratura i Prawo" Nr 9/2009, s. 148–154

[98] A. Lach: *Pojęcie posiadania pornografii dziecięcej w art. 202 § 4a kodeksu karnego w odniesieniu do danych informatycznych*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" Rok LXXII – Zeszyt 1 – 2010, s. 69–80

[99] A. Lach: *Prawnodowodowa problematyka zwalczania pedofilii i pornografii dziecięcej w internecie* [w:] *Materiały Seminarium Przestępczość Teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2004, s. 59–65.

[100] K. Liderman: *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?*, „Biuletyn Instytutu Automatyki i Robotyki" Nr 21/2004, WAT, Warszawa 2004

[101] K. Liderman: *O zagrożeniach dla skutecznej ochrony informacji, Przetwarzanej w sieciach i systemach teleinformatycznych, powodowanych nowomową*, Konferencja Cyberspace 2009, WAT, Warszawa 2009

[102] D. Lisiak-Felicka, M. Szmit: *„Tango Down" – Some Comments to the Security of Cyberspace of Republic of Poland* [w:] W. Biały, J. Kaźmierczak, *Systems supporting production engineering*, pod red. W. Białego, J. Kazimierczaka, PKJS, Gliwice 2012, s. 133–145

[103] T. Locher, P. Moor, S. Schmid, R. Wattenhofer: *Free Riding in BitTorrent is Cheap*, http://www.disco.ethz.ch/publications/hotnets06.pdf

[104] A. Lotko: *Źródła różnorodności informacji w marketingu relacyjnym*, „Studia i Materiały Wydziału Zarządzania UW" Nr 1/2007, s. 67–74, http://www.sim.wz.uw.edu.pl/pl/numer/numer-1-2007

[105] P. Lyman, H.R. Varian, J. Dunn, A. Strygin, K. Swearingen: *How Much Information 2000? University of Berkeley Raport, 2000*, http://www2.sims.berkeley.edu/research/projects/how-much-info/

[106] S. Łagodziński: *Przestępstwa przeciwko mieniu w kodeksie karnym (wybrane zagadnienia)*, „Prokuratura i Prawo" Nr 2/1999

[107] M. Maciejski: *Psychologiczna analiza sposobów przesłuchania świadków i reguł oceny ich zeznań w praktyce sędziowskiej a stopień przypisywanej im wiarygodności*, Katowice 2009, praca doktorska, maszynopis, http://www.sbc.org.pl/Content/19427/doktorat3009.pdf
[108] *Malarz Krzysztof Kuszej uniewinniony od zarzutu propagowania pedofilii*, http://wiadomosci.wp.pl/kat,1019395,title,Malarz-Krzysztof-Kuszej-uniewinniony-od-zarzutu-propagowania-pedofilii,wid,14791099,wiadomosc.html
[109] A. Malasińska-Nagórny: *Eksperyment prowadzony na podstawie art. 211 KPK a eksperyment rzeczoznawczy*, „Kwartalnik procesowo-kryminalistyczny" Nr 1-2 (10-11)/2012, Szkoła Policji w Pile, Piła 2012, http://pila.szkolapolicji.gov.pl/joomla/images/Zamowienia/Kwartalnik/Nr10-11/02eksperyment.pdf
[110] A. Marek: *Kodeks karny. Komentarz*, Wolters Kluwer, Warszawa 2007
[111] Z. Marek: *Błąd medyczny*, Wydawnictwo Medyczne, Kraków 2007
[112] Z. Marek: *Wybrane problemy opiniowania sądowo-lekarskiego*, Zakamycze, Kraków 2004
[113] J. Meteňko, K. Líška: *Riadenie operatívnych činností*, Akadémia Policajného Zboru, 2003
[114] J. Meteňko: *Možnosti A Využívanie KAI Technológii Pri Kontrole Závažnej Kriminality*, „Securitologia" Nr 6/2007, s. 112–118
[115] J. Meteňko, a kol: *Kriminalistické metódy a možnosti kontroly sofistikovanej kriminality*, Akademia PZ, Bratislava 2005
[116] A. Misiuk, P. Ciszek, J. Kosiński: *Przestępczość teleinformatyczna VI seminarium naukowe*, pod red. J. Kosińskiego, Wyższa Szkoła Policji, Szczytno 2003
[117] M. Molski, M. Łacheta: *Przewodnik audytora systemów informatycznych*, Helion, Gliwice 2007
[118] J. Moszczyński: *Standardy identyfikacji daktyloskopijnej*, „Problemy Kryminalistyki" Nr 261/2008, s. 14–21
[119] *Odpowiedź sekretarza stanu w Ministerstwie Sprawiedliwości – z upoważnienia ministra – na interpelację nr 15805 w sprawie internetowych przestępstw komputerowych*, http://orka2.sejm.gov.pl/IZ6.nsf/main/7B767D38
[120] Z. Okoń: *Komputerowe paragrafy – Program komputerowy w prawie autorskim*, „PCkurier" Nr 13/1998

[121] K. Pachnik: *Dowód z opinii biegłego w prawie polskim*, http://www.ora-warszawa.com.pl/uploaded/Dow%C3%B3d%20z%20opinii%20bieg%C5%82ego%20w%20prawie%20polskim.pdf

[122] K. Pachnik: *Prawne uwarunkowania odpowiedzialności cywilnej i karnej biegłych w polskim systemie prawnym*, „Edukacja Prawnicza" Nr 10 (118) / 2010, http://www.edukacjaprawnicza.pl/artykuly/artykul/a/pokaz/c/artykul/art/prawne-uwarunkowania-odpowiedzialnosci-cywilnej-i-karnej-bieglych-w-polskim-systemie-prawnym.html

[123] J.A. Pakuła: *Konta na serwerach gier internetowych w obrocie prawnym – zagadnienia węzłowe*, Warszawa 2009, praca magisterska, maszynopis http://prawo.vagla.pl/files/mgr_j_a_pakula.pdf

[124] N. Pamuła-Cieślak: *Zjawisko Ukrytego Internetu – rola bibliotek w upowszechnianiu jego zasobów, Materiały II Konferencja Biblioteki Politechniki Łódzkiej Biblioteki XXI wieku. Czy przetrwamy?*, s. 379–386, Łódź 2006, http://eprints.rclis.org/8925/1/pamula.pdf

[125] J. Paradysz, M. Szymkowiak: *Źródła danych ludnościowych Metodologia Badań Demograficznych*, Zeszyt nr 15. Sekcji Analiz Demograficznych PAN, s. 7–26, http://www.ae.krakow.pl/~demograf/Publikacje/SAD15.pdf

[126] *Perspectives of police science in Europe*, CEPOL 2007, https://www.cepol.europa.eu/fileadmin/website/Research_Science/PGEAPS_Final_Report.pdf

[127] A. Piaczyńska: *Posiadanie jako znamię czynu zabronionego*, „Prokuratura i Prawo" Nr 7–8/2010, s. 54–70

[128] H. Pietrzkowski: *Zarys metodyki pracy sędziego w sprawach cywilnych*, LexisNexis, Warszawa 2006

[129] M. Płachta: *Opinia w sprawie projektu ustawy o zmianie Kodeksu karnego, Kodeksu postępowania karnego oraz Kodeksu wykroczeń*, druk sejmowy nr 2031, Gdańsk 2004, http://orka.sejm.gov.pl/rexdomk4.nsf/(%24All)/4FC60869D85A3A73C1256E0B0047EE25/%24File/I2677-03b.rtf

[130] A. Płaza: *Przestępstwa komputerowe*, Rzeszów 2000, praca magisterska, maszynopis, http://vagla.pl/skrypts/mgr_a_plaza.pdf

[131] *Policja zajmuje się kradzieżą w wirtualnym świecie*, http://polska.newsweek.pl/policja-zajmuje-sie-kradzieza-w-wirtualnym-swiecie,62499,1,1.html

[132] V. Porada, K. Holcr, et al.: *Policejní vědy*, Vyd. Aleš Čeněk, Plzeň 2011
[133] *Prokuratura Okręgowa w Zielonej Górze: X Seminarium Kryminalistyczne „Kryminalistyka w Świecie Wirtualnej Zbrodni"* (Jesionka, 15–17 maja 2013 r.), http://zielona-gora.po.gov.pl/index.php?id=3&ida=10004
[134] W. Przybyło: *Postanowienie o dopuszczeniu dowodu z opinii biegłego w teorii i praktyce*, „Edukacja Prawnicza" z 13 października 2009 r., http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualnosc/art/postanowienie-o-dopuszczeniu-dowodu-z-opinii-bieglego-w-teorii-i-praktyce
[135] *Realni złodzieje w wirtualnych grach*, http://policyjni.gazeta.pl/Policyjni/1,103617,8779549,Realni_zlodzieje_w_wirtualnych_grach.html
[136] M.K. Rogers, J. Goldman, R. Mislan, T, Wedge: *Computer Forensics Field Triage Process Model*, *Conference on Digital Forensics, Security and Law, 2006*, http://www.digitalforensics-conference.org/CFFTPM/CDFSL-proceedings2006-CFFTPM.pdf
[137] P. Siemkowicz: *Przestępstwa o charakterze pedofilskim i przeciwko wolności seksualnej popełniane poprzez Internet, w ujęciu polskiego kodeksu karnego*, e-Czasopismo Prawa Karnego i Nauk Penalnych 7/2011, http://www.czpk.pl/artykuly/7-2011-Siemkowicz_P._Przestepstwa_o_charakterze_pedofilskim_i_przeciwko_wolnosci_seksualnej_popelniane_poprzez_Internet_w_ujeciu_polskiego_kodeksu_karnego.pdf
[138] P. Siemkowicz: *Przestępstwa skierowane przeciwko poufności, integralności i dostępności danych oraz systemów komputerowych w polskim kodeksie karnym – z uwzględnieniem aktualnych zmian nowelizacyjnych*, e-biuletyn CBKE, Wrocław 2009, http://www.bibliotekacyfrowa.pl/Content/34363/Przestepstwa_skierowane.pdf
[139] A. Siluszek: *Przestępstwa komputerowe*, „PCKurier" Nr 2000/8/42, http://www.pckurier.pl/archiwum/artykuly/siluszek_andrzej/2000_08_42/
[140] M. Siwicki: *Cyberprzestępczość*, C.H. Beck, Warszawa 2013
[141] A. Słodki: *W opinii biegłego – niewykonanie umowy w terminie*, „Nieruchomości" Nr 2(30)/2001
[142] M. Sowa: *Ogólna charakterystyka przestępczości internetowej*, „Palestra" Nr 5/6/2001 s. 25

[143] M. Sowa: *Przestępczość komputerowa – badanie celowości i skuteczności kryminalizacji*, Kraków 2005, praca doktorska, maszynopis, http://m-sowa.pl/MSowa-przestepczosc-komputerowa.pdf

[144] *Stanowisko Zespołu ds. Etyki w Nauce z 16 listopada 2000 r.*, Komitet Badań Naukowych, http://kbn.icm.edu.pl/etyka/praktyka.html

[145] B. Stefanowicz: *Informacja*, Oficyna Wydawnicza SGH, Warszawa 2004

[146] A. Strzelecki: *Legal Aspects of Deep Links on the Internet, Proceedings of the International Multiconference on Computer Science and Information Technology*, s. 559–563

[147] A. Suchecka-Tarnacka: *Biegły sądowy a prawidłowy wynik postępowania sądowego*, http://www.rozwiązywaniesporów.pl/2013/12/20/biegly-sadowy-a-prawidlowy-wynik-postepowania-sadowego

[148] A. Suchorzewska: *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer, 2010

[149] B. Sungarden: *An Infological Approach to Data Bases*, Ph.D. Thesis, https://sites.google.com/site/bosundgren/my-life/AnInfologicalApproachtoDataBases.pdf?attredirects=0

[150] A. Suworow, W. Krasucki: *Przestępcy specjalnej troski*, „Przegląd" Nr 36/2002, http://www.przeglad-tygodnik.pl/pl/artykul/przestepcy-specjalnej-troski-0

[151] K. Swearingen (ed.): *How Much Information 2003?*, University of Berkeley Raport, 2003, http://www2.sims.berkeley.edu/research/projects/how-much-info-2003

[152] M. Szmit, A. Baworowski, A. Kmieciak, P. Krejza, A. Niemiec: *Elementy Informatyki Sądowej*, pod red. M. Szmita, Polskie Towarzystwo Informatyczne, Warszawa 2011

[153] M. Szmit, M. Gusta, M. Tomaszewski: *101 zabezpieczeń przed atakami w sieci komputerowej*, Wydawnictwo Helion, Gliwice 2005

[154] M. Szmit, I. Politowska: *O artykule 267 Kodeksu Karnego oczami biegłego*, „Prawo Mediów Elektronicznych" (8), dodatek do „Monitora Prawniczego" Nr 16/2008, s. 34–40

[155] M. Szmit: *Bezpieczeństwo Informatyczne* [w:] I. Staniec, J. Zawiła-Niedźwiecki: *Zarządzanie ryzykiem operacyjnym*, s. 201–228, C.H. Beck, Warszawa 2008

[156] M. Szmit: *Biegły informatyk w postępowaniu cywilnym*, Zeszyty Naukowe Politechniki Łódzkiej, seria Elektryka z. 121, Nr 1078, s. 487–501, Łódź 2011
[157] M. Szmit: *Informatik jako expert v podmínkách polského legislativního system. Metodologické úvahy, Internet, Competitiveness and Organizational Security*, Tomas Bata University Zlín 2010
[158] M. Szmit: *Informatyka w Zarządzaniu*, Centrum Doradztwa i Informacji Difin Sp. z o.o., Warszawa 2003
[159] M. Szmit: *Kilka uwag o zadaniach biegłego informatyka w postępowaniu przygotowawczym w sprawach z art. 202 KK*, „Diariusz Prawniczy" Nr 16–17/2012, s. 97–108
[160] M. Szmit: *Z całą sumiennością i bezstronnością, czyli o informatyce sądowej*, „Magazyn Informatyki Śledczej" Nr 7/2010, s. 4–6, http://www.mediarecovery.pl/magazyn-is/magazyn_is_numer_7.pdf
[161] J. Śpiewak: *Wykorzystanie seksualne dziecka w kodeksie karnym od czerwca 2010 r.*, http://placzdziecka.blox.pl/html/1310721,262146,21.html?536592
[162] T. Tomaszewski: *Dowód z opinii biegłego w procesie karnym*, IES, Kraków 1998
[163] T. Tomaszewski: *Postanowienia o powołaniu biegłego w teorii i praktyce*, „Problemy Kryminalistyki" Nr 163/1984, s. 66–69
[164] N. Tuła: *Oględziny i ich rodzaje*, „Edukacja Prawnicza" z 17 września 2010 r., http://www.edukacjaprawnicza.pl/aktualnosci/a/pokaz/c/aktualnosc/art/ogledziny-i-ich-rodzaje.html
[165] J. Turek: *Biegły sądowy i jego czynności*, „Monitor Prawniczy" Nr 24/2007, s. 1358–1364
[166] S. Uhrín, P. Selinger: *Bezpečnostné služby*, Žilinská univerzita, 2003
[167] *Ukradł zbroję rycerzowi... z gry sieciowej*, http://krakow.gazeta.pl/krakow/1,44425,10655840,Ukradl_zbroje_rycerzowi____z_gry_sieciowej.html
[168] P. Waglowski: *Umowa o przeniesienie prawa do korzystania z awatarów i artefaktów*, http://prawo.vagla.pl/node/6065
[169] P. Waglowski: *Kradzież a usuwanie danych informatycznych – do Polski przybyły sprawy o „kradzież artefaktów" w grach MMORPG*, http://prawo.vagla.pl/node/9235"
[170] P. Waglowski: *And justice for all dot com*, http://prawo.vagla.pl/node/2858

[171] P. Waglowski: *Jak wynika z doniesień policji również bandyci grają w Tibia*, http://prawo.vagla.pl/node/9092
[172] P. Waglowski: *Nie można przełamać czegoś, co nie istnieje – polski wyrok w sprawie SQL Injection*, http://prawo.vagla.pl/node/8154
[173] P. Waglowski: *Projekt zmian kodeksu karnego pod internetową choinkę*, http://prawo.vagla.pl/node/9299
[174] P. Waglowski: *Secondlife: gdy organy ścigania stawiają zarzut za darmowy program*, http://prawo.vagla.pl/node/8138
[175] P. Waglowski: *Ukradli wirtualną broń*, http://prawo.vagla.pl/node/3212
[176] P. Waglowski: *Wirtualny miecz*, http://prawo.vagla.pl/node/188
[177] P. Waglowski: *Wyrok za słuchanie*, http://prawo.vagla.pl/node/5039
[178] J. Warylewski: *System Prawa Karnego. T. 10. Przestępstwa przeciwko dobrom indywidualnym*, pod red. J. Warylewskiego, Legalis, Warszawa 2012
[179] J. Warylewski: *Przestępstwo oszustwa komputerowego (art. 287 KK) — podstawowe zagadnienia teoretycznoprawne i praktyczne*, http://panda.bg.univ.gda.pl/%7Ewaryl/ok.htm
[180] J. Widacki: *Kryminalistyka*, pod red. J. Widackiego, C.H. Beck, Warszawa 2008
[181] J. Widacki: *Recenzja książki J. Wójcikiewicz: Eskpertyza sądowa*, „Palestra" 1,2/2003, http://palestra.pl/index.php?go=artykul&id=907
[182] T. Widła, M. Leśniak: *Chytrze bydlą z pany kmiecie*…, Międzynarodowa Konferencja z okazji 55-lecia powstania Laboratorium Kryminalistycznego KWP w Krakowie, http://konferencjalkkwp.weebly.com/abstrakty.html
[183] T. Widła: *Glosa do wyroku TK RP z 12 czerwca 2008 r., K 50/05*, „Palestra" Nr –7/8/2008, s. 291–301
[184] T. Widła: *Uwagi o przeprowadzaniu dowodu z opinii biegłych*, „Palestra" Nr 3 4/2002, s. 66–73
[185] T. Widła*: VAT-em biegłych, wystąpienie na 1 Kongresie Nauk Sądowych*, http://www.ptrm.pl/praktyka/warsztat-wyceny/informacja-z-przebiegu-pierwszego-kongresu-nauk-sadowych-w-warszawie
[186] L. Widmański: *Programy komputerowe i bazy danych jako samodzielne dobra na gruncie prawa polskiego – w szczególności w kontekście Internetu. Wybrane zagadnienia*, praca magisterska napisana na Wydziale Prawa

i Administracji Uniwersytetu Śląskiego w Katowicach, http://vagla.pl/skrypts/mgr_l_widmanski.pdf
[187] *Wielkopolska Grupa Prawnicza: Opinia biegłego pozasądowego w procesie cywilnym*, http://www.wgpr.pl/publikacje/77-opinia-bieglego-pozasadowego-w-procesie-cywilnym.html
[188] J. Wojtasik: *Akta sprawy jako materiał badawczy w ekspertyzie*, http://www.zielona-gora.po.gov.pl/index.php?id=36&ida=8265
[189] J. Wojtasik: *Eksperyment procesowo – kryminalistyczny*, http://www.zielona-gora.po.gov.pl/index.php?id=36&ida=2869
[190] J. Wójcikiewicz: *Ekspertyza sądowa*, Zakamycze, Kraków 2002
[191] J. Wójcikiewicz: *Metaopinie – wyraz siły czy słabości wymiaru sprawiedliwości, Biegły w sądzie (materiały konferencyjne)*, Wydawnictwo Instytutu Ekspertyz Sądowych, Kraków 2006 s. 103-106
[192] J. Wójcikiewicz: *Temida nad mikroskopem*, TNOiK, Toruń 2009
[193] W. Wróbel: *(Komentarze do art. 117–277 KK)* [w:] A. Zoll: *Kodeks karny. Część szczególna. Komentarz, T. II*, pod red. A Zolla, Zakamycze 2006, s. 1311–1314
[194] M. Wrześniewski: *Krytycznie o przestępstwach pornograficznych*, „Prokuratura i Prawo" Nr 11/2011, s. 98–111
[195] R. Zahorski: *Metodyka pracy biegłego sądowego. Rekonstrukcja wypadku drogowego*, Difin, Warszawa 2010
[196] M. Zalewski: *Cisza w sieci. Praktyczny przewodnik po pasywnym rozpoznawaniu i atakach pośrednich*, Helion, Gliwice 2005
[197] A. Zeliaś, B. Pawełek, S. Wanat: *Prognozowanie ekonomiczne,* Wydawnictwo Naukowe PWN, Warszawa 2003
[198] S. Ziemski: *Problemy dobrej diagnozy*, PWN, Warszawa 1973
[199] *Złodziej wirtualnych butów otrzymał prawomocny wyrok*, http://polygamia.pl/Polygamia/1,107162,8511906,Zlodziej_wirtualnych_butow_otrzymal_prawomocny_wyrok.html
[200] R. Zyzik: *Dowody neuronaukowe w polskim prawie dowodowym*, „Forum Prawnicze" vol. 2 (16)/2013, s. 23–34, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2337387
[201] K. Żaczkiewicz-Zborska: *Niedozwolony plik w koszu też jest karany*, http://www.lex.pl/czytaj/-/artykul/niedozwolony-plik-w-koszu-tez-jest-karany

[202] M. Żołna: *Kryteria oceny opinii biegłych*, „Problemy Kryminalistyki" Nr 259 (styczeń–marzec)/2008, s. 44–48
[203] M. Żołna: *Eksperyment procesowo-kryminalistyczny. Istota i dowodowa rola*, Diffin, Warszawa 2011
[204] A. Żygadło: *Pytania do i odpowiedzi biegłych sądowych* [w:] *IX seminarium naukowe*, Wyższa Szkoła Policji, Szczytno 2006, s. 173–190

Normy i standardy

[1] R. Shirey: RFC 2828, Internet Security Glossary, Network Working Group 2000, https://www.ietf.org/rfc/rfc2828.txt
[2] Przewodnik PKN-ISO Guide 73:2012 Zarządzanie ryzykiem Terminologia, PKN, Warszawa 2012
[3] Polska Norma PN-I-02000:2002 Technika informatyczna Zabezpieczenia w systemach informatycznych Terminologia, PKN, Warszawa 2002
[4] Polska Norma PN-ISO/IEC 2382-1:1996 Technika informatyczna Terminologia Terminy podstawowe, PKN, Warszawa 2001
[5] Polska Norma PN-ISO/IEC 2382-8:2001 Technika informatyczna Terminologia Bezpieczeństwo, PKN, Warszawa 2001
[6] Polska Norma PN-ISO/IEC 2382-14:2001 Technika informatyczna – Terminologia – Część 14: Niezawodność, obsługiwalność i dostępność, PKN, Warszawa 2001
[7] Polska Norma PN-I-13335-1:1999 Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych – Pojęcia i modele bezpieczeństwa systemów informatycznych, PKN, Warszawa 1999
[8] Polska Norma Polska Norma PN-ISO/IEC 17799:2007 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zarządzania bezpieczeństwem informacji, PKN, Warszawa 2007
[9] Polska Norma PN-EN ISO 19011:2012 Wytyczne dotyczące audytowania systemów zarządzania, PKN, Warszawa 2012
[10] Norma międzynarodowa ISO/IEC 27000:2014 Information technology – Security techniques – Information Security Management Systems – Overview and vocabulary, ISO 2014

[11] Norma międzynarodowa ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence, ISO 2012
[12] Norma międzynarodowa ISO 19011:2011 Guidelines for auditing management systems, ISO 2011
[13] Norma międzynarodowa ISO/IEC 17021:2011 Conformity assessment – Requirements for bodies providing audit and certification of management systems, ISO 2011

Strony www

[1] Bitthief, http://bitthief.ethz.ch
[2] DABI Sp. z o.o., http://www.dabi.pl
[3] Digital Universe Program, http://www.emc.com/leadership/programs/digital-universe.htm
[4] Dyżurnet NASK, http://www.dyzurnet.pl
[5] Helpline Fundacji Orange i Fundacji Dzieci Niczyje, http://helpline.org.pl
[6] Informatologia, http://hrcak.srce.hr/index.php?show=casopis&id_casopis=129&lang=en
[7] Kodeks Zawodowy Informatyków PTI, http://www.pti.org.pl/index.php/corporate/Kodeks-Zawodowy-Informatykow-PTI
[8] MediaRecovery, http://www.mediarecovery.pl
[9] Ministerstwo Sprawiedliwości Biuletyn Informacji Publicznej. Statystyki, http://bip.ms.gov.pl/pl/dzialalnosc/statystyki/
[10] Novell Audit, http://www.novell.com/poland/resourcecenter/novell_audit_charakterystyka_techniczna.pdf
[11] Policja. Statystyka. Kodeks karny, http://www.statystyka.policja.pl/st/kodeks-karny
[12] Pracownia Chemii Sądowej Uniwersytetu Jagiellońskiego, http://www2.chemia.uj.edu.pl/pracownia.php?id=10055
[13] Pracownia Informatyki Sądowej Instytutu Ekspertyz Sądowych, http://ies.krakow.pl/blog/struktura/pracownia-informatyki-sadowej/
[14] Sąd Okręgowy w Białymstoku. Informacje dla biegłych, http://bialystok.so.gov.pl/informacje/biegli.html

[15] Sąd Okręgowy w Bielsku-Białej. Informacje dla biegłych, http://www.bielsko-biala.so.gov.pl/biegli-sadowi,m,mg,3,24
[16] Stowarzyszenie Instytut Informatyki Śledczej. Najlepsze praktyki. Zabezpieczenia dowodów, http://www.siis.org.pl/najlepsze-praktyki/zabezpieczanie.html
[17] X-ways Forensics, http://www.x-ways.net/forensics/index-m.html

Wykaz powoływanych orzeczeń

Orzecznictwo Sądu Najwyższego

[1] Postanowienie Sądu Najwyższego z 11 kwietnia 1996 r. (I PRN 30/96, OSNAPiUS Nr 2/1997, poz. 28)
[2] Postanowienie Sądu Najwyższego z 7 listopada 2000 r. (I CKN 1170/98, OSNC Nr 4/2001, poz. 64)
[3] Postanowienie Sądu Najwyższego z 29 września 2004 r. (I KZP 21/04, OSNKW Nr 9/2004, poz. 90)
[4] Postanowienie Sądu Najwyższego z 25 czerwca 2003 r. (IV KK 8/03, OSNK Nr 1/2003, poz. 1355)
[5] Postanowienie Sądu Najwyższego z 7 listopada 2005 r. (V KK 91/05, OSNK Nr 1/2005, poz. 2005)
[6] Wyrok Sądu Najwyższego z 24 czerwca 1958 r. (IV KRN 170/58, NP Nr 2/1959, s. 249)
[7] Wyrok Sądu Najwyższego z 11 lipca 1969 r. (I CR 140/69, OSNCPiUS Nr 5/1970, poz. 85)
[8] Wyrok Sądu Najwyższego z 5 marca 1971 r., (I CR 593/70 OSNC Nr 12/1971, poz. 212)
[9] Wyrok Sądu Najwyższego z 12 listopada 1973 r. (II KR 285/72, OSNKW Nr 4/1974, poz. 73)
[10] Wyrok Sądu Najwyższego z 18 lipca 1975 r. (I CR 331/75, Legalis)
[11] Wyrok Sądu Najwyższego z 8 listopada 1976 r. (I CR 374/76, OSNCPiUS Nr 10/1997, poz. 187)
[12] Wyrok Sądu Najwyższego z 3 maja 1982 r. (I KR 319/81, OSNWPG Nr 11/1982, poz. 149)

[13] Wyrok Sądu Najwyższego z 10 maja 1982 r. (II KR 82/82, OSNKW Nr 10–11/1982, poz. 78)
[14] Wyrok Sądu Najwyższego z 7 lutego 1986 r. (IV KR 15/86, Legalis)
[15] Wyrok Sądu Najwyższego z 20 czerwca 1988 r. (I KR 174/88, OSNKW Nr 1112/1988, poz. 84)
[16] Wyrok Sądu Najwyższego z 10 grudnia 1998 r. (I CKN 922/97, Legalis)
[17] Wyrok Sądu Najwyższego z 19 maja 1998 r. (II UKN 55/98, OSNAPiUS Nr 10/1999, poz. 351)
[18] Wyrok Sądu Najwyższego z 29 lipca 1999 r. (II UKN 60/99, OSNAPiUS Nr 22/2000, poz. 831)
[19] Wyrok Sądu Najwyższego z 8 czerwca 2001 r. (I PKN 468/00, OSNAPiUS Nr 8/2003, poz. 197)
[20] Wyrok Sądu Najwyższego z 7 grudnia 2001 r. (IV KKN 563/97, OSNKW Nr 34/2002, poz. 17)
[21] Wyrok Sądu Najwyższego z 6 lutego 2003 r. (IV CKN 1763/00)
[22] Wyrok Sądu Najwyższego z 3 października 2003 r. (V KK 50/03, Legalis)
[23] Wyrok Sądu Najwyższego z 24 marca 2004 r. (IV KK 46/04, Legalis)
[24] Wyrok Sądu Najwyższego z 25 stycznia 2006 r. (I CK 281/05, Legalis)
[25] Wyrok Sądu Najwyższego z 19 października 2006 r. (V KK 221/06, Legalis)
[26] Wyrok Sądu Najwyższego z 14 marca 2007 r. (III UK 130/06, OSNAPiUS Nr 78, poz. 113)
[27] Wyrok Sądu Najwyższego z 7 października 2009 r. (III KK 122/09, Legalis)
[28] Wyrok Sądu Najwyższego z 3 lutego 2010 r. (II PK 192/09, Legalis)
[29] Wyrok Sądu Najwyższego z 24 sierpnia 2011r. (V KK 26/11)
[30] Wyrok Sądu Najwyższego z 19 grudnia 2012r. (II CNP 41/12, Legalis)
[31] Wyrok Sądu Najwyższego z 14 lutego 2013 r. (II CSK 371/12, Legalis)
[32] Uchwała Zgromadzenia Ogólnego Sądu Najwyższego z 15 lipca 1974 r. (Kw. Pr. 2/74, OSNCPiUS Nr 12/1974, poz. 203)
[33] Uchwała Pełnego Składu Izby Karnej Sądu Najwyższego z 25 czerwca 1980 r. (VII KZP 48/78, OSNKW Nr 8/1980, poz. 65)
[34] Uchwała Sądu Najwyższego z 30 października 1985 r. (III CZP 59/85, OSNCPiUS Nr 9/1986, poz. 140)

[35] Uchwała SN z 22 stycznia 2003 r. (I KZP 43/02, OSNKW Nr 12/2003, poz. 5)
[36] Uchwała Sądu Najwyższego z 17 lutego 2004 r. (III CZP 115/03, Legalis)

Orzecznictwo Naczelnego Sądu Administracyjnego

[37] Wyrok Naczelnego Sądu Administracyjnego z 20 sierpnia 1998 r. (II SA 992/98, „Monitor Prawniczy" Nr 8/1999)
[38] Uchwała Naczelnego Sądu Administracyjnego z 12 stycznia 2009 r. (I FPS 3/08, ONSAiWSA Nr 3/2009, poz. 46)
[39] Wyrok Naczelnego Sądu Administracyjnego Ośrodek Zamiejscowy w Łodzi z 20 maja 1997 r. (I SA/Łd 345/96)
[40] Wyrok Naczelnego Sądu Administracyjnego Ośrodek Zamiejscowy w Lublinie z 19 lutego 1999 r. (SA/Lu 43/98)
[41] Wyrok Naczelnego Sądu Administracyjnego z 4 czerwca 2001 r. (II SA 1434/00)
[42] Wyrok Naczelnego Sądu Administracyjnego Ośrodek Zamiejscowy w Łodzi z 3 października 2003 r. (I SA/Łd 2414/2001)
[43] Wyrok składu 7 sędziów Naczelnego Sądu Administracyjnego z 24 listopada 2003 r. (FSA 2/03, ONSA Nr 2, poz. 43)
[44] Wyrok Naczelnego Sądu Administracyjnego z 27 maja 2009 r. (II GSK 971/08)

Orzecznictwo Trybunału Konstytucyjnego

[45] Wyrok Trybunału Konstytucyjnego z 11 września 2007 r. (P 11/07, OTK Nr 8/2007, poz. 97)
[46] Wyrok Trybunału Konstytucyjnego z 23 kwietnia 2008 r. (SK 16/07, OTK Nr 3/2008, poz. 45)
[47] Wyrok Trybunału Konstytucyjnego z 12 czerwca 2008 r. (K 50/05, OTK Nr 6/2008, poz. 111)

Orzecznictwo Sądów Apelacyjnych

[48] Postanowienie Sądu Apelacyjnego we Wrocławiu z 19 stycznia 2012 r. (II A Kz 23/12) niepubl.
[49] Postanowienie Sądu Apelacyjnego w Krakowie z 13 lutego 2012 roku (Acz 164/12)
[50] Postanowienie Sądu Apelacyjnego w Katowicach z 21 czerwca 2012 r. (II AKz 386/12)
[51] Wyrok Sądu Apelacyjnego w Lublinie z 10 lipca 2003 r. (II Aka 107/03)
[52] Wyrok z 11 maja 2005 r. Sądu Apelacyjnego w Poznaniu (I ACa 1875/04)
[53] Wyrok Sądu Apelacyjnego we Wrocławiu z 5 września 2012 r. (II AKa 155/12)
[54] Wyrok Sądu Apelacyjnego we Wrocławiu z dnia 27 września 2012 roku (II AKa 171/12)

Orzecznictwo Wojewódzkch Sądów Administracyjnych

[55] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 12 maja 2008 r. (II SA/WA 326/08)
[56] Wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z 11 marca 2009 r. (II SA/Wr 251/08)

Orzecznictwo Sądu Najwyższego USA

[57] Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993) http://supreme.justia.com/cases/federal/us/509/579/case.html
[58] Daubert v. Merrell Dow Pharmaceuticals, Inc., 43 F. 3d 1311 – Court of Appeals, 9th Circuit 1995, http://law.justia.com/cases/federal/appellate-courts/F3/43/1311/552448
[59] General Electric Co. v. Joiner, 522 U.S. 136 (1997) http://supreme.justia.com/cases/federal/us/522/136/case.html
[60] Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999) http://supreme.justia.com/cases/federal/us/526/137/case.html

Wykaz skrótów

Akty prawne

[1] DRASI – Decyzja Ramowa Rady Europy 2005/222/WSiSW z 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dziennik Urzędowy Unii Europejskiej L 69/67 z 16.3.2005)

[2] DRRESWD – Decyzja Ramowa Rady Europy 2004/68/WSiS z 22.12. 2003 r. o zwalczaniu seksualnego wykorzystywania dzieci i pornografii dziecięcej (Dziennik Urzędowy Unii Europejskiej L 013 z 20. 01.2004 r.)

[3] DZNTCS – Dyrektywa Parlamentu Europejskiego i Rady 2011/92/UE z 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej (Dziennik Urzędowy Unii Europejskiej L 335 z 17.12.2011)

[4] KK – ustawa z 6 czerwca 1997 r. – Kodeks karny (Dz.U. 1997 Nr 88, poz. 553 z późn. zm.)

[5] KodEL – Kodeks Etyki Lekarskiej – uchwała Nadzwyczajnego II Krajowego Zjazdu Lekarzy z 14 grudnia 1991 z późn. zm.; dostępny na: http://www.nil.org.pl/__data/assets/pdf_file/0003/4764/Kodeks-Etyki-Lekarskiej.pdf

[6] KPA – ustawa z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t. jedn.: Dz.U. z 2013 r., poz. 267)

[7] KPC – ustawa z 17 listopada 1964 r. – Kodeks postępowania cywilnego (t. jedn.: Dz.U. z 2014 r., poz. 101)

[8] KPK – ustawa z 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz.U. 1997 r. Nr 89, poz. 555 z późn. zm.)

[9] KREoC – Konwencja Rady Europy o cyberprzestępczości, Budapeszt 2001 (ETS No. 185)

[10] KREODSW – Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, Lanzarote 2007, (CETS No. 201)

[11] KW – ustawa z 20 maja 1971 r. – Kodeks wykroczeń (t. jedn.: Dz.U. z 2013 r., poz. 482

[12] PrAut – ustawa z 4 lutego1994 r. o prawie autorskim i prawach pokrewnych (t. jedn.: Dz. U. Nr 90, poz. 631)

[13] PrTel – ustawa z 16 lipca 2004 r. – Prawo telekomunikacyjne (t. jedn. Dz.U. z 2014 r., poz. 243)

[14] RoBS – rozporządzenie Ministra Sprawiedliwości z 24 grudnia 1928 r. o biegłych sądowych (Dz.U. z 1928 r. Nr 104, poz. 945).

[15] RKZIS – rozporządzenie Ministra Pracy i Polityki Społecznej z 27 kwietnia 2010 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz jej stosowania (Dz.U. Nr 82, poz. 537)

[16] RORRKZ – rozporządzenie Ministra Handlu Wewnętrznego i Usług z 23 kwietnia 1983 r. w sprawie oznaczania rodzajów rzemiosł, określenia uprawnień i kwalifikacji zawodowych wymaganych do ich wykonywania oraz pierwszeństwa kombatantów w uzyskiwaniu zezwoleń na wykonywanie rzemiosła (Dz.U. z 1983 r., Nr 22, poz. 98).

[17] ROWDN – rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z 8 sierpnia 2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych (Dz.U. z 2011 r. Nr 179, poz. 1065)

[18] RWCKPIST – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych (Dz.U. z 2010 r. Nr 177, poz. 1195).

[19] RwsBS – rozporządzenie Ministra Sprawiedliwości z 24 stycznia 2005 r. w sprawie biegłych sądowych (Dz.U. z 2005 r. Nr 15, poz. 133)

[20] UBRIS – ustawa o biegłych rewidentach i ich samorządzie (Dz.U. z 2009 r. Nr 77, poz. 649)

[21] UCKSST – Uchwała Centralnej Komisji do Spraw Stopni i Tytułów z 28 stycznia 2011 r. zmieniającą uchwałę w sprawie określenia dzie-

dzin nauki i dziedzin sztuki oraz dyscyplin naukowych i artystycznych (M.P. Nr 14/2011 r., poz. 149)
[22] ULS – ustawa z 15 czerwca 2007 r. o lekarzu sądowym (Dz.U. z 2007 r. Nr 123, poz. 849)
[23] UOBD – ustawa o ochronie baz danych z 27 lipca 2001 r. (Dz.U. z 2001 r. Nr 128, poz. 1402 z późn. zm.)
[24] UODO – ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych (t. jedn.: Dz. U. Nr 101, poz. 926)
[25] UOFP – ustawa z 27 sierpnia 2009 r. o finansach publicznych (t. jedn.: Dz.U. z 2013 r., poz. 885)
[26] UOINF – ustawa z 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t. jedn.: Dz.U. z 2013 r., poz. 235)
[27] UON – ustawa z 20 września 2002 r. o normalizacji (Dz.U. z 2002 r. Nr 169, poz. 1386 z późn. zm.)
[28] UONUDE – ustawa z 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. z 2002 r. Nr 126, poz. 1068)
[29] UOSP – ustawa z 29 czerwca 1995 r. o statystyce publicznej (t. jedn.: Dz.U. z 2012 r. poz. 519 z późn. zm.)
[30] UPEA – ustawa z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji (t. jedn.: Dz.U z 2012 r., poz. 1015)
[31] UŚUDE – ustawa z 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r., poz. 1422)
[32] UUSW – ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. Nr 64, poz. 565, z późn. zm.)
[33] UzmKK – ustawa z 4 kwietnia 2014 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2014 r., poz. 538)
[34] UzmwCUJ – ustawa z 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. Nr 171, poz. 1056)
[35] Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483 z późn. zm.)

[36] Federalna Reguła Dowodowa 702 (Sąd Najwyższy USA 2011), http://www.law.cornell.edu/rules/fre/rule_702
[37] I poprawka do Konstytucji Stanów Zjednoczonych, http://www.law.cornell.edu/anncon/html/amdt1afrag1_user.html#amdt1a_hd4
[38] VII poprawka do Konstytucji Stanów Zjednoczonych, http://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-8.pdf

Inne skróty

art. – artykuł
ang. – angielski
C/S – Client/Server
CD – Compact Disk
CIA – Confidentionality, Integrity, Availability
dosł. – dosłownie
DVD – Digital Versatile Disc
ed. – editor
etc. – et caetera (i tak dalej)
gr. – grecki
ibid. – ibidem (tamże)
IEC – International Electrotechnical Commission
IEEE – The Institute of Electrical and Electronics Engineers
IETF – Internet Engineering Task Force
IP – Internet Protocol
ISO – International Organization for Standardization
itd. – i tak dalej
itp. – i temu podobne
ITU-T – International Telecommunication Union – Telecommunication Standardization Sector
łac. – łacina
MAC – (1) Media Access Control;
– (2) Modification, Last Access, Creation Times
NASK – Naukowa Akademicka Sieć Komputerowa
nast. – następne

np. – na przykład
NNTP – Network News Transfer Protocol
op. cit. – opere citato (z cytowanego dzieła)
P2M – peer-to-mail
PN – Polska Norma
PKN – Polski Komitet Normalizacyjny
por. – porównaj
późn. – późniejszy
przyp. aut. – przypis autora
r. – rozdział
s. – strona
tj. – to jest
z. – zeszyt
zm. – zmiana
zob. – zobacz

ERRATA
do książki „Wybrane zagadnienia opiniowania sądowo-informatycznego”

Ważniejsze błędy dostrzeżone w druku

Strona	**Wiersz**	**Jest**	**Powinno być**
111	15 od dołu w prawej kolumnie tabeli	łoletniego poniżej lat 15, podlega karze	łoletniego, podlega karze
166	5 od dołu w przypisie 374	piętnasty	osiemnasty

Dr Maciej Szmit jest członkiem Rady Biegłych przy Sądzie Okręgowym w Łodzi, rzeczoznawcą Polskiego Towarzystwa Informatycznego oraz jednym z redaktorów tematycznych w półroczniku „Securitologia" wydawanym wspólnie przez Collegium Civitas i European Association for Security. Zawodowo pracuje w Orange Labs, w Wydziale Bezpieczeństwa IT dla Korporacji na stanowisku starszego kierownika projektu, gdzie zajmuje się zarządzaniem ryzykiem bezpieczeństwa informacji w projektach teleinformatycznych realizowanych w krajach Europy i Afryki. Jest autorem i współautorem kilkudziesięciu artykułów i kilku książek poświęconych różnym aspektom zarządzania bezpieczeństwem informacji, między innymi: „101 zabezpieczeń przed atakami w sieci komputerowej" (Helion 2005), „13 najpopularniejszych ataków na twój komputer. Wykrywanie, usuwanie skutków i zapobieganie" (Helion 2008), „Elementy informatyki sądowej" (PTI 2011), „Ćwiczenia laboratoryjne z bezpieczeństwa systemów sieciowych" (Wydawnictwo PŁ 2011) oraz problematyce pogranicza informatyki i zarządzania: „Zarządzanie projektem. Wybrane metody i techniki" (Horyzont 2003), „Informatyka w Zarządzaniu" (Difin 2003).

Kraków 2014

ISBN 978-83-61645-10-8