AUTOMATYKA • 2008 • Tom 12 • Zeszyt 3

Dominika Lisiak*, Izabela Politowska**, Maciej Szmit*

Ignorantia iuris nocet. Świadomość prawnych aspektów użytkowania komputerów wśród informatyków

1. Przedmiot i cel badania

W polskim systemie prawnym zagadnienia dotyczące użytkowania komputerów zawarte są w wielu różnych ustawach i rozporządzeniach, których interpretacja jest często niejednoznaczna i kłopotliwa. Jak się wydaje, spora część przestępstw komputerowych popełniana jest z powodu braku znajomości lub złej interpretacji obowiązujących przepisów. Choć zagadnienia dotyczące prawa komputerowego powinny być znane w szczególności informatykom, to w praktyce spora część z nich nie ma, albo co gorsza – ma błędne pojęcie o obowiązujących przepisach.

W niniejszym tekście przedstawione są wyniki pilotażowego badania ankietowego, które przeprowadzone zostało wśród nauczycieli akademickich i studentów informatyki. Celem badania było poznanie wiedzy oraz poglądów i opinii dotyczących praktycznych aspektów użytkowania systemów informatycznych w świetle polskich standardów normatywnych.

2. Metoda badania

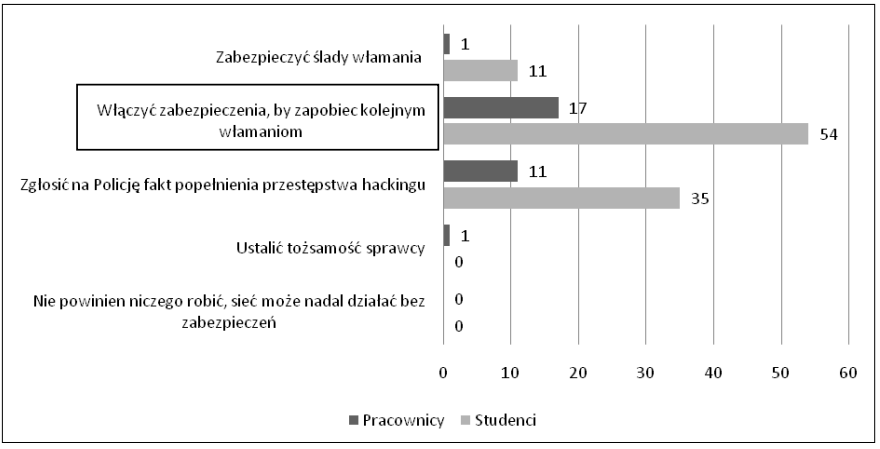
W ramach badania przeprowadzono pisemną ankietę wśród pracowników Katedry Informatyki Stosowanej oraz studentów kierunku Informatyka na Wydziale Elektrotechniki Elektroniki Informatyki i Automatyki, Politechniki Łódzkiej (III, IV i V rok studiów dziennych magisterskich oraz I rok studiów zaocznych). Dobór próby (zobacz także [16, s. 48–60]) podyktowany był przede wszystkim dostępnością badanych i możliwością uzyskania stosunkowo wysokiej responsywności. Badanie ankietowe nie spełnia zatem wymogów metody reprezentacyjnej, dlatego jego wyników nie można interpretować jako opinii zbiorowości generalnej (porównaj [8, s. 200–241]). Ogółem rozdano 148 ankiet i uzyskano 130 poprawnie wypełnionych zwrotów.

* Katedra Informatyki Stosowanej, Politechnika Łódzka
** Katedra Prawa Międzynarodowego Publicznego i Stosunków Międzynarodowych, Uniwersytet w Łodzi

Ankieta była anonimowa i składała się z dziewięciu pytań. Pytania miały charakter zamknięty. Pięć z nich (pierwsze cztery i ostatnie) były pytaniami dysjunktywnymi, pozostałe cztery pytania były pytaniami koniunktywnymi. Pytania występujące w ankiecie opracowano na podstawie wytycznych, które można znaleźć w literaturze przedmiotu [9, s. 53–73], [15, s. 66–120]. Oprócz pytań weryfikujących wiedzę i opinie na temat zagadnień z zakresu szeroko rozumianego prawa komputerowego (pytania 1–8) zostało umieszczone jedno pytanie (pytanie 9) dotyczące poglądów ankietowanych na temat stopnia jego restrykcyjności.

3. Wyniki

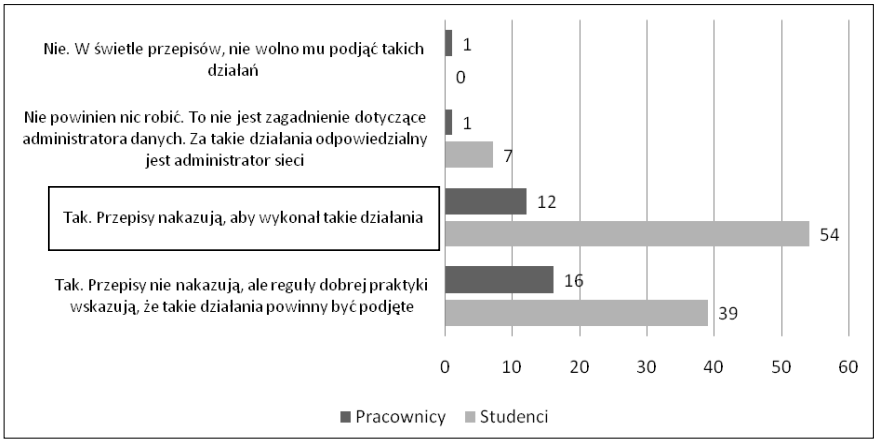
Na wykresach (rys. 1–9) przedstawione zostały ilości odpowiedzi na poszczególne pytania z podziałem na nauczycieli akademickich oraz studentów informatyki. Prawidłowe odpowiedzi zostały oznaczone ramkami. Jakkolwiek – z uwagi na stosunkowo dużą liczebność próby – otrzymane wyniki można uznać za nieźle oddające poglądy pracowników i studentów, to – z uwagi na niezachowanie wymogów metody reprezentacyjnej – nie można ich uogólnić, co było zresztą zgodne z założeniami badania, które miało mieć charakter pilotażowy. Zwraca uwagę, że w niektórych przypadkach (najczęściej dla pytania nr 1) zaznaczono więcej niż jedną (mimo wyraźnego komentarza) wymaganą odpowiedź (łącznie w 12 przypadkach). Takie przypadki zostały odrzucone i nie były brane pod uwagę przy dalszych analizach wyników.



Rys. 1. Odpowiedzi pracowników i studentów na pytanie 1: „W firmie FIRMA ABC od tygodnia funkcjonuje nowa sieć komputerowa, która nie została jeszcze zabezpieczona. W tym czasie dokonano włamania do systemu i przechwycono ważne dla firmy informacje (niebędące jednak informacjami szczególnie chronionymi). Co Pani/Pana zdaniem powinien zrobić administrator sieci? (proszę zaznaczyć 1 odpowiedź, którą uważa Pani/Pan za słuszną)”
Źródło: opracowanie własne

Na pytanie dotyczące włamania do niezabezpieczonej sieci większość ankietowanych, zarówno pracowników (17 osób), jak i studentów (54 osoby), zaznaczyła odpowiedź prawidłową, tj. włączenie zabezpieczeń, aby zapobiec dalszym włamaniom. Jednakże, dość duża grupa osób (11 pracowników i 35 studentów) zaznaczyła odpowiedź, że miało miejsce w tym przypadku przestępstwo hackingu. Natomiast 11 studentów i 1 pracownik sugeruje zabezpieczenie śladów włamania.

Komentarz: Zgodnie z brzmieniem art. 267 § 1 polskiego kodeksu karnego [1] karalne jest uzyskanie informacji przez osobę, która nie była uprawniona do jej posiadania, a jednym ze sposobów uzyskania tejże informacji może być przełamanie elektronicznych zabezpieczeń. Przepis mówi wyłącznie o uzyskaniu informacji poprzez przełamanie, nieominięcie zabezpieczeń, choć w praktyce ustalenie, czy mamy do czynienia z przełamaniem czy ominięciem może nie być takie proste. Czyn ten określany jest mianem tzw. przestępstwa hackingu. Podkreślić należy, iż stawia się wymóg faktycznego zabezpieczenia informacji. Jeśli włamanie do sieci nastąpiło w momencie, w którym (choćby na krótko) zabezpieczenie nie było aktywne – nie można mówić o popełnieniu przestępstwa [18, s. 1279], nie ma zatem sensu zgłaszania zawiadomienia o przestępstwie ani zabezpieczanie śladów włamania (przynajmniej nie dla celów dowodowych, może jedynie dla poznawczych).

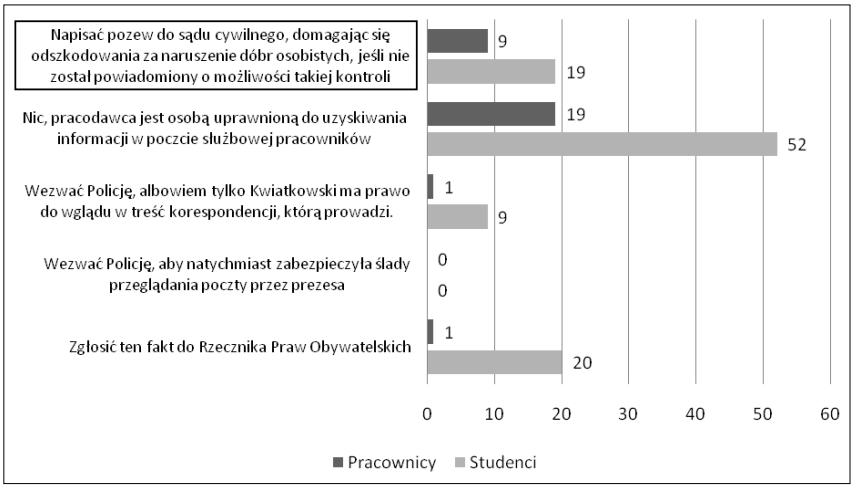


Rys. 2. Odpowiedzi pracowników i studentów na pytanie 2: „W instytucji XYZ dane osobowe są przechowywane i przetwarzane w systemie informatycznym, który jest połączony z siecią publiczną. Czy Pani/Pana zdaniem, administrator danych powinien zabezpieczyć pomieszczenia, w których przetwarzane są dane, przed dostępem osób nieuprawnionych oraz kontrolować przepływ informacji pomiędzy systemem informatycznym a siecią publiczną? (proszę zaznaczyć 1 odpowiedź, która jest według Pani/Pan za słuszną)"
Źródło: opracowanie własne

W przypadku odpowiedzi na pytanie dotyczące obowiązków administratora danych większość studentów (54 osoby) zaznaczyła odpowiedź prawidłową, natomiast 39 studentów uważa, że działania te nie są nakazane przepisami prawa, a jedynie reguły dobrej

praktyki wskazują, że powinny być podjęte. Wśród pracowników wyniki wynoszą odpowiednio 12 i 16.

Komentarz: Zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych obowiązki administratora danych w zakresie zapewnienia zabezpieczenia danych osobowych zawarte są w art. 36–39a ustawy [2]. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed dostępem osób nieuprawnionych oraz ich zmianą, utratą, uszkodzeniem lub zniszczeniem (art. 36.1). Podkreślić należy, iż w rozumieniu art. 7 pkt. 4)[4] ustawy [2] administratorem danych jest organ, jednostka organizacyjna, podmiot lub osoba (spośród wymienionych art. 3 ustawy), decydująca o celach i środkach przetwarzania danych osobowych. Na mocy delegacji zawartej w art. 39a ustawy zostały w rozporządzeniu szczegółowo określone podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych [3]. Wśród wymienionych szczegółowo w załączniku do rozporządzenia obowiązków zapewnienia bezpieczeństwa informacji są wymóg fizycznego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe [3, załącznik do rozporządzenia – część A. Środki bezpieczeństwa na poziomie podstawowym, pkt. I.1.] oraz kontrola przepływu informacji pomiędzy systemem informatycznym a siecią publiczną [3, Załącznik do rozporządzenia – część C. Środki bezpieczeństwa na poziomie wysokim, pkt. XII.2.b). Są to obowiązki administratora danych – odpowiedzią prawidłową jest więc odpowiedź nr 3.



Rys. 3. Odpowiedzi pracowników i studentów na pytanie 3: „Prezes Kowalski skontrolował zawartość służbowej poczty elektronicznej pracownika Kwiatkowskiego. Co według Pani/Pana powinien zrobić Kwiatkowski w obronie swojej prywatności? (proszę zaznaczyć 1 odpowiedź, którą uważa Pani/Pan za wskazaną)"

Źródło: opracowanie własne

W odniesieniu do pytania nr 3, 19 ankietowanych pracowników uważa, że pracodawca jest osobą uprawnioną do uzyskiwania informacji w poczcie służbowej pracowników, to samo potwierdza 52 studentów. Z kolei 9 pracowników i 19 studentów ma zdanie, że jeśli pracownik nie został powiadomiony o możliwości takiej kontroli, to może napisać pozew do sądu cywilnego domagając się odszkodowania za naruszenie dóbr osobistych. Natomiast 20 studentów sądzi, że taką sprawą powinien zająć się Rzecznik Praw Obywatelskich.

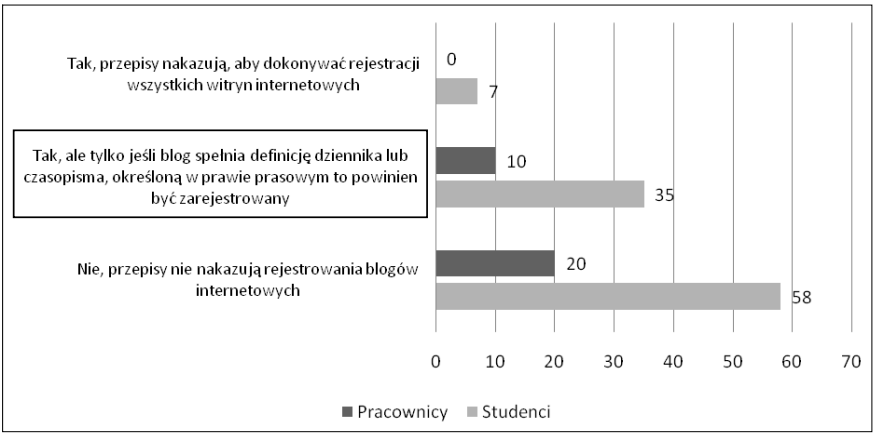
Komentarz: Prawo wglądu pracodawcy w treść służbowej poczty elektronicznej pracownika należy rozpatrywać na dwóch płaszczyznach: potencjalnej odpowiedzialności karnej pracodawcy i potencjalnej odpowiedzialności cywilnej [12].

W odniesieniu do tej pierwszej kwestii należy przyjąć, iż pracownik z pewnością nie korzysta z prawnokarnej ochrony treści elektronicznej korespondencji służbowej. Wskazuje na to analiza art. 267 § 1 k.k. Artykuł ten penalizuje uzyskanie informacji przez osobę nieuprawnioną poprzez podłączenie się do przewodu służącego do przekazywania informacji lub poprzez przełamanie elektronicznego, magnetycznego lub innego szczególnego zabezpieczenia. Po pierwsze pracownicy mają założone i prowadzone konta pocztowe na serwerze należącym do pracodawcy przez podlegającego mu administratora systemu informatycznego, który wydaje hasła dostępu do skrzynek pocztowych. Do zapoznania się z treścią listów elektronicznych nie jest więc konieczne przełamanie zabezpieczeń elektronicznych ani żadnych innych specjalnych zabezpieczeń, jest ona dostępna dla pracodawcy bezpośrednio. A skoro nie ma przełamania zabezpieczeń, nie można mówić o popełnieniu przestępstwa z art. 267 § 1. Wyjątek może stanowić szczególna sytuacja, w której wiadomości są zaszyfrowane z użyciem specjalnego programu i ich odczytanie nie jest możliwe bez przełamania szczególnego zabezpieczenia. Przestępstwo zostaje jednak popełnione, gdy w wyniku przełamania zabezpieczenia dostęp do informacji uzyskała osoba do tego nieuprawniona. Treść korespondencji służbowej pracownika powinna pozostawać w związku z zakresem jego obowiązków służbowych, jest dokonywana w imieniu pracodawcy i pozostaje w sferze jego interesów. Pracodawca jest więc osobą uprawnioną do zapoznania się z treścią informacji i nie popełnia przestępstwa określonego w art. 267 § 1.k.k. [10].

Odnośnie do ochrony prawa do prywatności i tajemnicy korespondencji pracownika, a więc potencjalnej odpowiedzialności odszkodowawczej pracodawcy na gruncie prawa cywilnego za naruszenie tych dóbr, to sprawa nie jest do końca przesądzona i budzi wiele emocji, w zależności od grupy interesów, która jest reprezentowana [17, s. 217–220], [11]. Najbardziej przejrzystym rozwiązaniem dla obu stron byłoby wcześniejsze uprzedzenie pracowników przez pracodawcę o możliwości stosowania kontroli służbowej korespondencji elektronicznej. Rzecznik Praw Obywatelskich Janusz Kochanowski skierował do minister pracy i polityki społecznej list, w którym zwrócił uwagę na coraz częściej stosowaną i na coraz szerszą skalę praktykę kontroli korespondencji elektronicznej pracowników oraz potrzebę uprzedzania ich o takim zamiarze przez pracodawców. Brak uprzedzenia pracownika o możliwości takiej kontroli może narazić pracodawcę na zarzut naruszenia dóbr osobistych pracownika i zarazem stwarza pracownikowi możliwość ewentualnego docho-

dzenia odszkodowania w procesie cywilnym. Zaakcentował to niedawno Europejski Trybunał Praw Człowieka w wyroku z 3 kwietnia 2006 w sprawie Copland przeciwko Wielkiej Brytanii (no. 62617/00).

Za prawidłowe w świetle prawnych wymogów możliwości kontroli poczty służbowej przez pracodawcę przy pytaniu nr 3 uznać możnaby zarówno odpowiedź pierwszą, jak i drugą. W treści pytania odnieśliśmy się jednak do możliwości ochrony prawa do prywatności przez pracownika, a więc chodziło o wskazanie, czy pracownik potencjalnie mógłby i w pod jakimi warunkami dochodzić ochrony swoich praw czując się pokrzywdzony ich naruszeniem. Odpowiedzią prawidłową jest odpowiedź pierwsza.



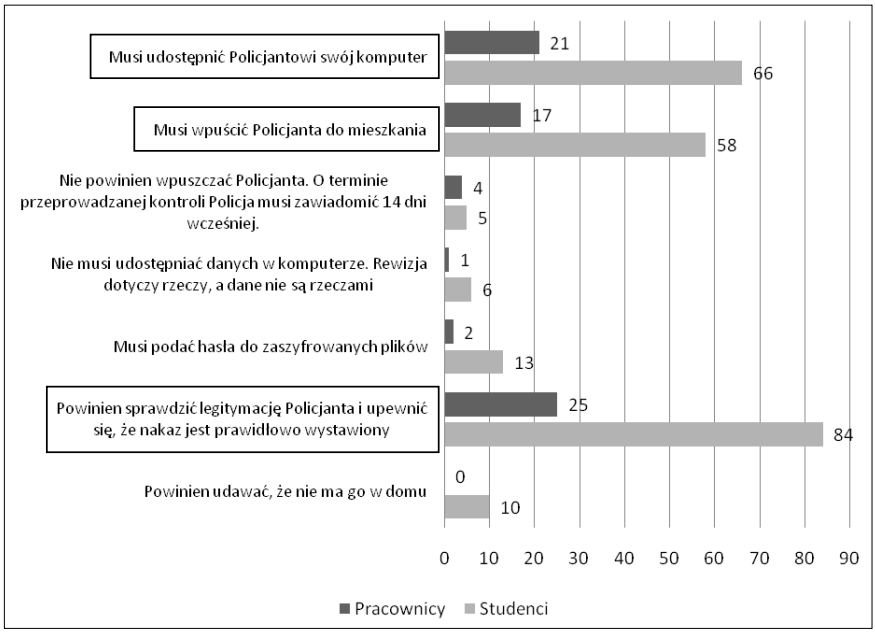
Rys. 4. Odpowiedzi pracowników i studentów na pytanie 4: „Pani Kowalska prowadzi swój blog internetowy. Czy Pani/Pana zdaniem powinna go zarejestrować? (proszę zaznaczyć 1 odpowiedź, którą uważa Pani/Pan za słuszną)"
Źródło: opracowanie własne

Na pytanie dotyczące konieczności zarejestrowania blogu internetowego 20 pracowników i ponad połowa studentów uważa, że przepisy nie nakazują takiej czynności. Pozostali pracownicy i 35 studentów uważa, że należy dokonać rejestracji blogu, tylko jeśli spełnia on definicję dziennika lub czasopisma, określoną w prawie prasowym. Wśród studentów znalazło się 7, którzy stwierdzili, że przepisy nakazują dokonywania rejestracji.

Komentarz: Problem uznania stron internetowych za czasopisma i obowiązku ich rejestracji w świetle wynikającego z art. 45 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe [4] budził wiele kontrowersji. Wynikały one z prób interpretacji ustawowej definicji prasy zawartej w art. 7 ust. 2 pkt. 1 prawa prasowego. Za rozstrzygające w tej kwestii należy uznać postanowienie Sądu Najwyższego z dnia 26 lipca 2007 r. (sygn. akt. IV KK 174/2007), zgodnie z którym „prasą są zarówno dzienniki i czasopisma, jak i wszelkie istniejące i powstające w wyniku postępu technicznego środki masowego przekazywania (…) upowszechniające publikacje periodyczne za pomocą druku, wizji, fonii lub innej techniki

rozpowszechniania." W związku z tym, gdy przekaz istnieje tylko w formie elektronicznej w Internecie, ale ukazuje się periodycznie, spełniając wymogi, o których mowa w art. 7 ust. 2 pkt. 1 prawa prasowego, istnieje obowiązek jego rejestracji, niedopełnienie którego skutkować może odpowiedzialnością karną z art. 45 prawa prasowego. Odpowiedzią prawidłową jest odpowiedź nr 2.

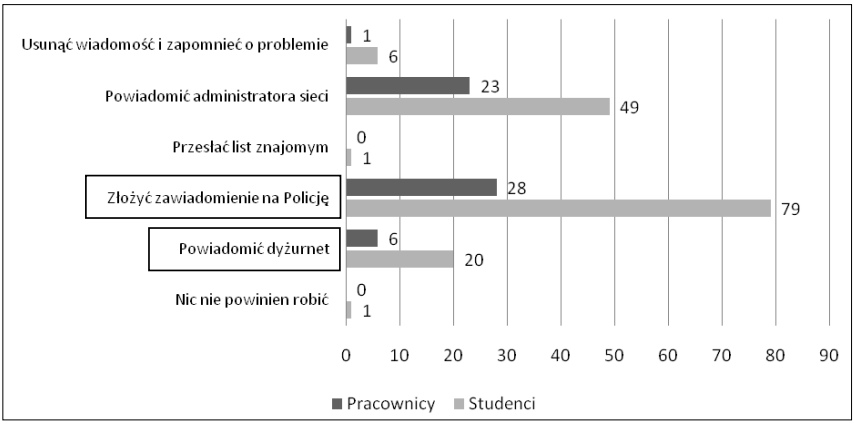
Kolejne 4 pytania dawały możliwość wybrania kilku odpowiedzi.



Rys. 5. Odpowiedzi pracowników i studentów na pytanie 5: „Do mieszkania Pana Malinowskiego puka Policjant, który chce sprawdzić legalność oprogramowania zainstalowanego w jego komputerze. Posiada ze sobą nakaz sądowy. Co Pani/Pana zdaniem musi lub powinien zrobić Malinowski? (proszę zaznaczyć wszystkie odpowiedzi, które uważa Pani/Pan za słuszne)"
Źródło: opracowanie własne

Podczas przeprowadzania kontroli oprogramowania w mieszkaniu, zarówno studenci jak i pracownicy najpierw sprawdziliby legitymację policjanta i nakaz sądowy lub prokuratorski. Kolejne odpowiedzi, które uzyskały dużą liczbę głosów, to odpowiedzi wskazujące na udostępnienie policjantowi komputera oraz wpuszczenie policjanta do mieszkania. Można zauważyć, że 13 studentów i 2 pracowników podałoby hasła do zaszyfrowanych plików, 10 studentów udawałoby, że nie ma ich w domu, a 5 studentów i 4 pracowników nie wpuściłoby policjanta bez wcześniejszej zapowiedzi o przeprowadzaniu kontroli. W sumie 6 studentów i 1 pracownik uważają, że nie należy udostępniać danych w komputerze, bo dane nie są rzeczami, a rewizja dotyczy rzeczy.

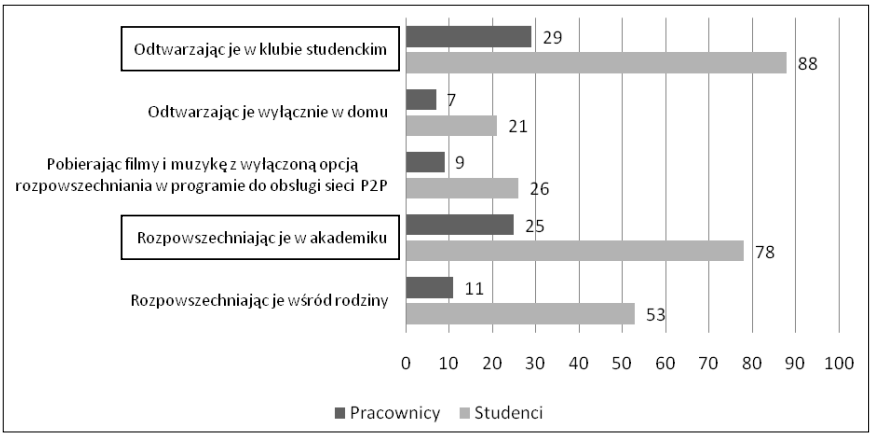
Komentarz: Przeszukanie pomieszczeń i innych miejsc może nastąpić w celu znalezienia rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że wymienione rzeczy tam się znajdują (art. 219 kodeksu postępowania karnego [5]). Postanowienie sądu lub prokuratora należy okazać osobie, u której przeszukanie ma być przeprowadzone (art. 220 § 2 k.p.k.). Osobie, u której przeszukanie ma nastąpić, jak najbardziej przysługuje więc prawo upewnienia się, iż został wydany nakaz oraz sprawdzenia legitymacji policjanta – i takich prawidłowych odpowiedzi uzyskano przy tym pytaniu najwięcej. Po sprawdzeniu nakazu (albo jak ktoś woli bez jego sprawdzenia), powinniśmy wpuścić policjanta do mieszania, odpowiedź nr 2 jest również odpowiedzią prawidłową. Istnieją w tym zakresie pewne reguły dotyczące dokonywania przeszukania pomieszczeń zamieszkałych w porze dziennej, czyli między 6 rano a 22 wieczorem, ale w wypadkach niecierpiących zwłoki przeszukanie może nastąpić również w porze nocnej (art. 221 § 1 oraz 2 k.p.k). Na tej samej podstawie należy uznać, że osoba, u której ma nastąpić przeszukanie, musi udostępnić w tym celu swój komputer – przeszukanie może dotyczyć „pomieszczeń i innych miejsc" i przyjmuje się interpretację, że zwrot ten odnosi się do systemu komputerowego [14]. Podobnie w celu odnalezienia plików mogących stanowić dowód popełnienia przestępstwa można przeprowadzić przeszukanie systemu informatycznego lub jego części, a więc należy udostępnić dane w komputerze (odpowiedź 3). Nie jest natomiast wymagane podawanie haseł do zaszyfrowanych plików – osoba kontrolowana może odmówić składania takich zeznań, zwłaszcza, jeśli podanie ich naraziłoby ją na odpowiedzialność karną. Nie ma także prawnego obowiązku wcześniejszego uprzedzenia o dokonaniu przeszukania. Zatem prawidłowe działania określają odpowiedzi nr 1, 2 i 6.



Rys. 6. Odpowiedzi pracowników i studentów na pytanie 6: „Pan Nowak otrzymał wiadomość e-mail z linkiem do strony, na której znajdują się zdjęcia z dziecięcą pornografią. Co Pani/Pana zdaniem powinien zrobić Pan Nowak? (proszę zaznaczyć wszystkie odpowiedzi, które uważa Pani/Pan za wskazane)"
Źródło: opracowanie własne

Odpowiedzi na pytanie dotyczące maila z dziecięcą pornografią przedstawiały się następująco. W dużej większości zarówno studenci, jak i pracownicy zgłosiliby ten fakt na policję. Znacząca część powiadomiłaby administratora sieci. Z kolei 6 pracowników i 20 studentów wysłałoby zgłoszenie do dyżurnetu, a 6 studentów i 1 pracownik wolałoby usunąć wiadomość i zapomnieć o problemie. Tylko jedna osoba nie podjęłaby żadnych działań.

Komentarz: Zgodnie z art. 202 § 3 k.k. rozpowszechnianie lub publiczna prezentacja treści pornograficznych z udziałem małoletniego jest przestępstwem zagrożonym karą pozbawienia wolności od 6 miesięcy do lat 8. Karalne jest także utrwalanie treści pornograficznych z udziałem małoletniego oraz ich sprowadzanie, przechowywanie lub posiadanie (art. 202 § 4 i 4a k.k.). Z uwagi na wysoką szkodliwość społeczną czynu osoba posiadająca na ten temat informacje powinna złożyć zawiadomienie o podejrzeniu popełnienia przestępstwa – odpowiedź prawidłowa nr 4, wybrana przez większość respondentów. Zawiadomienie o przestępstwie nie jest w tym przypadku obowiązkiem prawnym, a jedynie społecznym, więc jego realizacja wynikać będzie z postawy przyjętej przez osobę posiadającą informację. Istnienie zespołów takich jak dyżurnet.pl umożliwia internaucie szybką i łatwą reakcję na zauważony problem, nie jest to jednak wykorzystanie dostępnych środków prawnych. Można jednak uznać powiadomienie dyżurnetu za również poprawną odpowiedzią na pytanie 6.

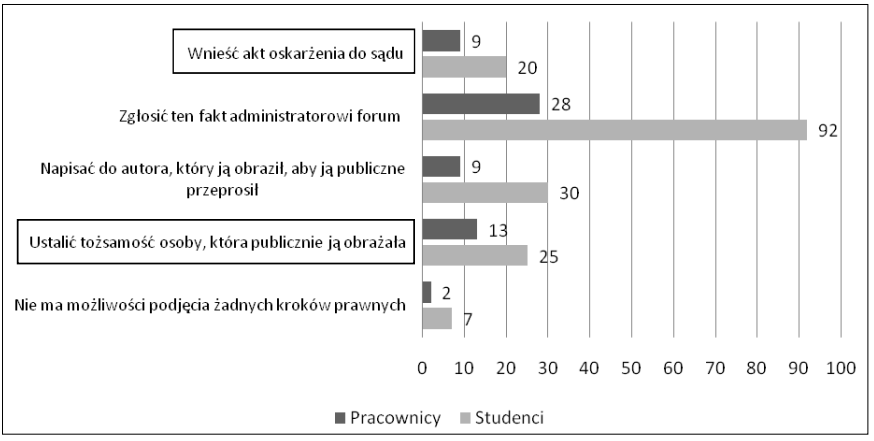


Rys. 7. Odpowiedzi pracowników i studentów na pytanie 7: „Student Miśkiewicz pobiera za pomocą programu do obsługi sieci P2P filmy, utwory muzyczne. W którym przypadku Pani/Pana zdaniem naruszy prawo? (proszę zaznaczyć wszystkie odpowiedzi, które uważa Pani/Pan za słuszne)"
Źródło: opracowanie własne

Na pytanie dotyczące pobierania utworów muzycznych i filmów najwięcej ankietowanych uważa, że łamie przepisy w przypadku publicznego odtwarzania w klubie studenckim, Kolejne przypadki, w których zdaniem ankietowanych łamane jest prawo to: rozpowszechnianie utworów w akademiku – 25 pracowników i 78 studentów, rozpowszechnianie

wśród rodziny – 11 pracowników i 53 studentów. Pozostałe odpowiedzi uzyskały porównywalną liczbę głosów w obu badanych grupach.

Komentarz: Konstrukcja dozwolonego użytku prywatnego wynikająca z art. 23 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych [6] daje możliwość korzystania z pojedynczych egzemplarzy rozpowszechnionych już utworów w zakresie swojego użytku osobistego oraz przez krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego [13, s. 147]. Z kolei w odniesieniu do art. 116 wymienionej ustawy nie jest dozwolone rozpowszechnianie cudzych utworów, ale dozwolone jest pobieranie rozpowszechnionych już utworów. Odpowiedzi prawidłowe dla pytania szóstego to odpowiedź nr 1 i 4 – w tych wypadkach nastąpi naruszenie prawa.

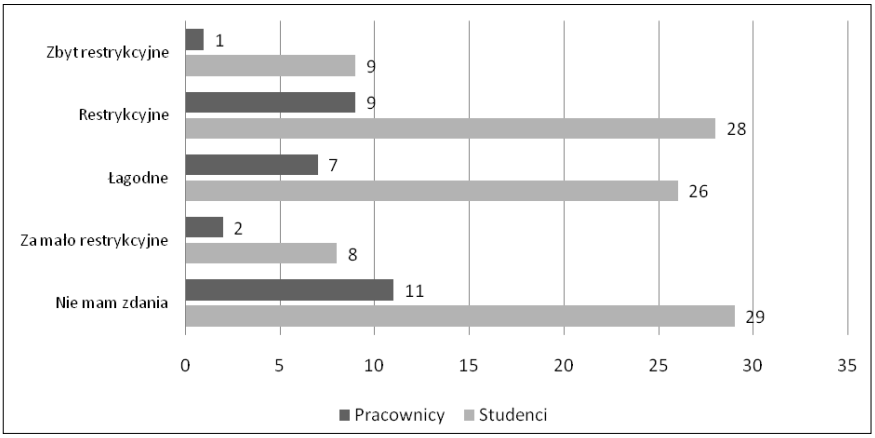


Rys. 8. Odpowiedzi pracowników i studentów na pytanie 8.: „Pani Kowalska zauważyła, że na forum internetowym, z którego korzysta, jeden z jego uczestników anonimowo przesyła posty, w których obraża ją, używając słów niecenzuralnych. Co Pani/Pana zdaniem powinna zrobić, aby pociągnąć autora wpisów do odpowiedzialności karnej? (proszę zaznaczyć wszystkie odpowiedzi, które uważa Pani/Pan za wskazane)"
Źródło: opracowanie własne

W ósmym pytaniu dominującą odpowiedzią wśród studentów i pracowników była odpowiedź dotycząca zgłoszenia faktu publicznej obrazy do administratora forum. Porównywalne wyniki otrzymały odpowiedzi o publicznych przeprosinach, ustaleniu tożsamości osoby obrażającej i wniesieniu aktu oskarżenia. Najmniejsza grupa ankietowanych uważa, że nie ma możliwości podjęcia jakichkolwiek działań prawnych.

Komentarz: Przestępstwa zniesławienia (art. 212 § 4 k.k.) i zniewagi (art. 216 § 5 k.k.) są przestępstwami ściganymi z oskarżenia prywatnego, co oznacza, że aby pociągnąć sprawcę do odpowiedzialności karnej, pokrzywdzony powinien wszcząć postępowanie karne, wnosząc prywatny akt oskarżenia do sądu. Akt ten musi określać osobę oskarżonego, określać czyn mu zarzucany i wskazywać dowody, na których opiera się oskarżenie. Prawi-

dłowe odpowiedzi w tym pytaniu odpowiedź nr 1 w połączeniu z odpowiedzią nr 4, gdyż aby wnieść prywatny akt oskarżenia pokrzywdzony musi najpierw ustalić tożsamość sprawcy. Zgłoszenie problemu administratorowi może wprawdzie być skuteczne z praktycznego punktu widzenia, ewentualnie może dopomóc w ustaleniu rzeczywistej tożsamości sprawcy, nie jest jednak środkiem prawnym.



Rys. 9. Odpowiedzi pracowników i studentów na pytanie 9: „Polskie prawo karne komputerowe uważa Pani/Pan za (proszę zaznaczyć 1 odpowiedź, którą uważa Pani/Pan za słuszną)"
Źródło: opracowanie własne

Ostatnie pytanie dotyczyło oceny restrykcyjności prawa komputerowego. Zdania były podzielone i zarówno opcje restrykcyjne, jak i łagodne otrzymały porównywalne wyniki. Nie można wskazać odpowiedzi dominującej. Aż 11 pracowników i 29 studentów nie ma zdania na ten temat.

4. Wnioski

Do ankiety wybranych zostało kilka zupełnie praktycznych sytuacji, w których elementarne poczucie etyki podpowiada człowiekowi, że jedno zachowanie jest naganne a inne – pożądane. Niestety przepisy polskiego prawa – z uwagi na stopień komplikacji, a niejednokrotnie również przez nieprecyzyjną redakcję i różnorodną ich wykładnię – wymagają czasem podjęcia zupełnie nieintuicyjnych (przynajmniej dla informatyka) działań. Prawo polskie jest trudne i mało czytelne, a niejednokrotnie również bardziej restrykcyjne niż w innych krajach. Jego znajomość jest dla informatyków jednak bardzo pożyteczna, a nieznajomość może prowadzić do przykrych konsekwencji.

Analizując wyniki badań, można zauważyć, że zarówno studenci, jak i pracownicy mają zbliżone poglądy na temat zagadnień poruszanych w ankiecie. Jednak w obrębie każdego pytania istnieją duże rozbieżności w odpowiedziach.

Pozytywnie należy ocenić fakt, iż w pytaniu 1. większość respondentów w obydwu badanych grupach zaznaczyła odpowiedź prawidłową, chociaż niemała grupa pozostaje w przekonaniu, iż zostało popełnione przestępstwo hackingu i należy zawiadomić o tym odpowiednie organy ścigania. Jak się wydaje, mając do wyboru jedynie jedną prawidłową odpowiedź, informatycy wybrali najbardziej intuicyjne rozwiązanie (włamanie-przestępstwo-zawiadomić policję). Dodatkowo w przekonaniu tym utwierdza fakt, że w pytaniu wielokrotnie zaznaczono więcej niż jedną prawidłową odpowiedź. Większość spośród aktualnie bądź potencjalnie wykonujących zawód administratora sieci ma świadomość faktu, że zaniedbanie z ich strony poprzez nieprawidłowe zabezpieczenie systemu skutkować może także niemożnością ścigania sprawcy incydentu.

W odniesieniu do wyników odpowiedzi na pytanie nr 2, odpowiedź prawidłową wskazało większość ankietowanych, co może być spowodowane powszechną świadomością informatyków o ochronie danych osobowych. Część ankietowanych uważa jednak, że sposób zabezpieczenia powinien być zapewniony regułami dobrej praktyki, co nie jest wystarczające. Wynikać to może z poczucia ich etyki (zwłaszcza pracowników).

Z odpowiedzi na pytanie nr 3 widać, że ankietowani albo nie są w większości zdeterminowani do poszukiwania ochrony ewentualnego naruszenia prawa do prywatności i tajemnicy korespondencji przez pracodawcę, albo nie mają świadomości możliwości podjęcia takich działań (dominuje odpowiedź nr 2). Większy procent pracowników niż studentów podjęłoby działanie zmierzające do ochrony tego dobra (odpowiedź nr 1).

Dane dotyczące odpowiedzi na pytanie czwarte wskazują, że większość spośród ankietowanych w obydwu grupach nieświadomie może narazić się na odpowiedzialność karną wynikającą z obowiązku rejestracji periodycznie uzupełnianego blogu internetowego. Może to wynikać z faktu, iż dopiero w ostatnim czasie sprawa ta została przesądzona mocą postanowienia Sądu Najwyższego. Prowadzenie blogów internetowych jest dość powszechną formą aktywności użytkowników w Internecie, należałoby więc dołożyć starań w celu w celu upowszechnienia tej informacji.

Zaskakujące są rozbieżności dotyczące odpowiedzi na pytanie nr 5, czyli to, że większość respondentów wpuściłaby policjanta do mieszkania po okazaniu przez niego legitymacji służbowej i nakazu przeszukania, ale nie przekłada się to na gotowość umożliwienia dokonania przeszukania. Odpowiedź dotyczącą udawania, iż nikogo nie ma w domu, umieściliśmy raczej z powodów humorystycznych, ale okazuje się, iż i takie postawy (wśród studentów) mogą się zdarzyć.

Z odpowiedzi uzyskanych na pytanie nr 6 można wywnioskować, iż problem pornografii dziecięcej budzi na tyle negatywne emocje, iż większość respondentów zdecydowałaby się powiadomić Policję o fakcie otrzymania odsyłacza do takich materiałów. Część osób przedsięwzięłaby mniej radykalne działanie, mianowicie powiadomiła administratora sieci bądź dyżurnet. Zaledwie w kilku przypadkach ankietujący wykazaliby się bierną postawą.

Wydaje się być uprawnionym twierdzenie, że występują problemy z interpretacją prawa autorskiego, ponieważ w pytaniu nr 7 uzyskano wiele poprawnych odpowiedzi, ale

znaczna część jest także niepoprawnych i użytkownicy nie do końca mają świadomość, które działania podejmowane przez nich mogą być zgodne z prawem, a które nie.

Informatycy nie wiedzą także co zrobić, by móc pociągnąć sprawcę zniesławienia do odpowiedzialności karnej – dokładnie tak brzmiało pytanie. Większość zgłosiłaby ten fakt administratorowi forum, co może być rozwiązaniem praktycznym, ale nie wiąże się z bezpośrednią możliwością pociągnięcia sprawcy do odpowiedzialności karnej.

Rozbieżności w uzyskanych odpowiedziach na pytanie 9 oraz duża ilość odpowiedzi „nie mam zdania" wskazują na niewystarczającą znajomość i małe zainteresowanie informatyków zagadnieniami prawa komputerowego.

Podsumowując wyniki badania należy stwierdzić, iż:

- Nie ma większych różnic pomiędzy wiedzą z zakresu prawa między grupą studentów a grupą pracowników naukowych.
- W niektórych pytaniach da się zauważyć skrajnie różne odpowiedzi, co wskazuje, że być może są one udzielane intuicyjnie, przy czym intuicja dość często zawodzi. Wydaje się, że przyczyną takiego stanu rzeczy może być z jednej strony brak dostatecznego zainteresowania tematem, z drugiej zaś fakt, iż prawo komputerowe jest rozproszone w różnych aktach prawnych, co utrudnia zapoznanie się z nim, a dodatkowo informatykom trudno może być zrozumieć treść formułowanych w języku prawnym przepisów.
- Należałoby rozważyć wprowadzenie do programu studiów informatycznych przedmiotu (choćby jako wykład fakultatywny) dotyczącego podstaw prawa komputerowego. Obecnie w ramach studiów kierunku informatyka na Wydziale Elektrotechniki Elektroniki Informatyki i Automatyki prowadzone są przedmioty: prawo gospodarcze (IX semestr studiów dziennych magisterskich) oraz prawo inżynierskie i ochrona własności intelektualnej (studia stacjonarne i niestacjonarne I stopnia). Jeśli wprowadzenie nowego przedmiotu nie byłoby możliwe to należałoby rozważyć przynajmniej możliwość rozszerzenia zakresu obowiązujących przedmiotów o zagadnienia dotyczące prawa komputerowego. Można również rozpatrzeć możliwość zaproszenia specjalistów w dziedzinie cyberprzestępczości, którzy w ramach wykładów mogliby przedstawić studentom te zagadnienia z praktycznego punktu widzenia.
- Informatycy powinni we własnym zakresie zapoznać się z wybranymi przepisami prawa, bo leży to w ich własnym interesie.

Literatura

Przepisy prawne

[1] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 1997 r., Nr 88, poz. 553 z późn. zm.).

[2] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.).

[3] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r., Nr 100, poz. 926).

[4] Ustawa z dnia 26 stycznia 1984 r. Prawo prasowe (Dz. U. z 1984, Nr 5, poz. 24 z późn. zm.).
[5] Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 1997 r., Nr 89, poz. 555).
[6] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Tekst jedn. Dz. U. z 2006 r., Nr 90, poz. 631).

Publikacje

[7] Adamski A., *Prawo karne komputerowe*. Warszawa, 2000, 45–55.
[8] Babbie E., *Badania społeczne w praktyce*. Wydawnictwo Naukowe PWN 2003, 200–241.
[9] Babiński G., *Pytania kwestionariuszowe: podstawowe podziały i typologie*. [w:] J. Wasilewski (red.), Wybrane zagadnienia metodologiczno-teoretyczne badań socjologicznych.
[10] Bajończyk A., *Karnoprawne aspekty ochrony prawa pracownika do komunikowania się*. Cz. II, Palestra, 2003, z. 3–4.
[11] Chadkowski M., Ciszek P., *Tajemnica korespondencji pracownika a ochrona tajemnicy handlowej pracodawcy*. Monitor Prawa Pracy, Nr 1/2007.
[12] Dulewicz K., *Czy pracodawca może kontrolować pracownika*. Gazeta Prawna, Nr 219/2007.
[13] Golat R., *Prawo autorskie i prawa pokrewne*. Warszawa, 2006.
[14] Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*. Prokuratura i Prawo, 2003/10/16 – t. 8.
[15] Lutyńska K., *Wywiad kwestionariuszowy. Przygotowanie i sprawdzenie narzędzia badawczego*. Ossolineum, 1984, 66–120.
[16] Szreder M., *Metody i techniki sondażowych badań opinii*. Polskie Wydawnictwo Ekonomiczne 2004, 48–60.
[17] Waglowski P., *Prawo w sieci*. Gliwice, 2005, 217–220.
[18] Zoll A. (red.), Wróbel W., *Kodeks karny. Część szczególna*. Komentarz, T. II, Zakamycze 2006, 1279–1284.