

Przedmowa

Dokładnie 20 lat temu, w 1998 r., została w Polsce opublikowana praca prof. *Janusza Barty* i prof. *Ryszarda Markiewicza* „Internet a prawo” (*J. Barta, R. Markiewicz, Internet a prawo, Kraków 1998, s. 3 i nast.*), poświęcona wpływowi nowego (w tamtym czasie) medium, czyli Internetu, na ówczesne prawo. Autorzy zaprezentowali w niej kierunki zmian dotyczących prawa prasowego, prawa cywilnego, własności intelektualnej, prawa pracy czy prawa podatkowego. Pojawiły się w niej także interesujące pytania – jak bardzo duży wpływ na nas, na prawo i jego stosowanie będzie miał Internet. Warto umiejscowić to w odpowiednim kontekście i przypomnieć sobie, że był to czas początków: telefonii komórkowej (Centertel uruchomił swoje usługi w 1992 r., a Era i Plus pojawiły się dopiero w 1996 r.) pierwszych, prostych, statycznych stron internetowych, prostych maili z załącznikami o wielkości zaledwie kilku kilobajtów, SMS-ów do 160 znaków bez multimediiów itd. Dzienniki Ustaw były wówczas publikowane na papierze, a systemy informacji prawniczej dopiero raczkowały.

Zaledwie (albo aż) 20 lat później funkcjonujemy w zupełnie innym świecie, gdzie w naszym codziennym życiu mamy do czynienia z zaawansowanymi portalami społecznościowymi, bankowością elektroniczną, smartfonami, które swoją mocą przewyższają tysiące razy moc obliczeniową komputerów sprzed 20 lat, kryptowalutami, *YouTubem*, *streamingiem on-line*, technologią *blockchain* wypierającą coraz częściej usługi prawników, chmurowym (w telefonie komórkowym) podpisem elektronicznym, chmurą obliczeniową i przechowywanymi w niej danymi, treściami cyfrowymi, własnością wirtualną, kreatorami umów, sztuczną inteligencją analizującą np. stan prawny, orzecznictwo oraz stan faktyczny, potrafiącą przewidzieć z olbrzymią pewnością orzeczenia. Brzmi jak inna epoka? Zdecydowanie! A to

przecież jeszcze nie wszystkie innowacje. Obecnie wdrażane są projekty związane z pojazdami autonomicznymi (m.in. samochody, drony towarowe, drony osobowe), rozwijana jest technologia Internetu rzeczy (mieliśmy już pierwsze ataki na systemy teleinformatyczne z użyciem procesorów w urządzeniach takich jak ekspresy, telewizory). Domowe i biurowe urządzenia same się porozumiewają, ściągają dane, wysyłają je, często wpływają na nasze zachowanie (np. nowoczesne samochody). Pojawiają się także nowe czyny zabronione (przestępstwa?) nieznanne dotychczasowym regulacjom karnym, np. „przejęcie” awatara w grze komputerowej, artefaktów i innych elementów tzw. „własności wirtualnej”, często o wielotysięcznej wartości, niekoniecznie wyrażanej w tradycyjnych jednostkach pieniężnych, ale np. w kryptowalutach.

Za tymi wszystkimi zmianami próbuje też nadążyć legislacja. Mamy już więc gotowe lub będące w przygotowaniu regulacje o charakterze europejskim oraz transgranicznym dotyczące nowych technologii, usług z nimi związanych, danych, treści cyfrowych itd. Mowa tu na przykład o RODO, e-Privacy, NIS, eIDAS, PSD2 w zakresie bankowości, rozporządzeniu o geoblokowaniu, uznaniu bitcoina jako środka płatniczego w niektórych systemach, dopuszczeniu w kilku państwach do ruchu drogowego w pełni autonomicznych pojazdów czy też praktycznym wykorzystaniu technologii *blockchain* do autentykacji transakcji. Widoczne jest zmniejszanie roli państw na rzecz technologii i społeczeństwa informacyjnego.

Minęło zaledwie 20 lat... Gdzie będziemy za kolejne 20?

Cyfryzacja w istotny sposób wpływa na społeczeństwo i na każdego człowieka z osobna. Zmieniają się sposoby zachowania i komunikowania, w tym dokonywanie czynności prawnych, często w sposób tak łatwy jak nigdy wcześniej (wystarczy kilka kliknięć, aby dokonać czynności prawnej łącznie z realizacją płatności). Coraz większego znaczenia nabiera także wymiar międzynarodowy, a co za tym idzie – prawo prywatne międzynarodowe i kwestia jurysdykcji. W obrocie wzrasta rola reguł *soft law*, zastępując twarde regulacje. I w tym wszystkim musi odnaleźć się prawnik – zarówno jako profesjonalista wspierający wyżej wskazane procesy, jak i osądający spory, a także jako zwykły użytkownik systemów teleinformatycznych.

Niniejsza publikacja ma na celu przybliżenie tej ostatniej roli, tj. prawnika jako użytkownika systemów teleinformatycznych, wypełniającego przynajmniej w minimalnym zakresie wymagania prawne związane z jego funkcjonowaniem w środowisku elektronicznym.

Praktycznie nie jest możliwe działanie współczesnego prawnika bez komputera, telefonu komórkowego czy też poczty elektronicznej. Wielu korzysta także z narzędzi, takich jak komunikatory (często darmowe), narzędzia chmurowe, niejednokrotnie nie zdając sobie sprawy zarówno z wymogów prawa, jak i zasad bezpieczeństwa związanych z ich używaniem. Nieszyfrowanie dysków, pendrive'ów, wiadomości wychodzących z poczty elektronicznej, przechowywanie danych na serwerach w „dziwnych” państwach, brak odpowiednich fizycznych zabezpieczeń (np. szafek na serwery, komputery), wadliwe administrowanie dostępem do danych, urzędzeń – niestety nie należą do rzadkości. Często, znając tylko z teorii nowe narzędzia informatyczne, takie jak kwalifikowane pieczęcie elektroniczne lub usługi zaufania – prawnicy nie do końca wiedzą, jak je mogą wykorzystać w swojej codziennej pracy. Poważny problem może też sprawić wdrożenie w kancelarii wszystkich wymogów zawartych w RODO, w szczególności dotyczących przechowywania danych w postaci elektronicznej, w tym w chmurze, spełnienie wymogów prawa do bycia zapomnianym czy też przenoszalności danych.

Publikacja ta przybliży powyższą problematykę, przede wszystkim zaś pomaga w zrozumieniu, a zatem też spełnieniu wymogów RODO odnoszących się do przechowywania danych w kancelarii.

Praca składa się z trzech części.

Pierwsza, o charakterze monografii, wskazuje na: zasady odpowiedzialności dyscyplinarnej radcy prawnego oraz adwokata za naruszenie przepisów korporacyjnych, w tym etyki; zasady odpowiedzialności karnej oraz cywilnej związanej z wykorzystywaniem i naruszeniem bezpieczeństwa IT; kwestie, w jaki sposób przechowywać dane osobowe w ramach RODO i projektowanej ustawy o ochronie danych osobowych w kancelarii prawnej; jak zastosować w systemach kancelaryjnych zasadę *privacy by design* wynikającą z RODO i jakie są konsekwencje naruszenia tego obowiązku; wreszcie relacji danych IT z prawem właściwym, m.in. jakie są konsekwencje kolizyj-

noprawne zainstalowania chmurowego Windowsa 365, poczty *Gmail* czy darmowego *Dropboxa*.

Druga część jest rodzajem poradnika, w ramach którego prezentowane są regulacje prawne, ale także zasady bezpieczeństwa w zakresie zabezpieczeń fizycznych kancelarii i dostępu do urządzeń IT; zabezpieczania systemów, zasady bezpiecznego korzystania z poczty elektronicznej; sieci Internet; reguły robienia kopii zapasowych, zasady i wymogi prawne dotyczące stron internetowych kancelarii; przechowywania danych kancelarii w chmurze (rodzaje chmury).

Trzecia część przybliży najnowsze, ogólnie dostępne aplikacje do wykorzystania w kancelarii prawnej, jak również reguły prawne ich dotyczące. Są to: portal informacyjny, portal orzeczeń, elektroniczne postępowanie upominawcze, elektroniczne poświadczenie odbioru czy też wykorzystanie kwalifikowanego podpisu elektronicznego. W tej części można znaleźć zarówno reguły prawne, praktyczne omówienie, jak i grafiki pokazujące, jak korzystać z danej aplikacji.

W imieniu całego zespołu autorskiego życzymy przyjemnej i pożytecznej lektury.

prof. UO dr hab. *Dariusz Szostek*
Krzysztof Kamiński

mec. *Jacek Pawłowski*
mec. *Cezary Żelaźnicki*
Kancelaria PwC Legal