Ochrona konkurencji i konsumentów a unijny model cyberbezpieczeństwa
(od redaktorów)

Bezpieczeństwo cyberprzestrzeni od lat pozostaje jednym z obszarów szczególnego zainteresowania zarówno ze strony instytucji i organów Unii, jak i poszczególnych państw członkowskich. Wieloaspektowość problematyki cyberbezpieczeństwa powoduje, że zagadnienie to rozważane jest coraz częściej nie tylko w obszarze ochrony kluczowych systemów i sieci informatycznych, lecz także z perspektywy wpływu na rynek ochrony konkurencji i konsumentów. Dowodem aktualności tej problematyki jest zakończona w 2019 roku zawarciem ugody precedensowa sprawa *FTC v D-Link*, w ramach której amerykański organ ochrony konkurencji skutecznie dowodził, że wprowadzenie na rynek tzw. usieciowionych produktów konsumenckich nieposiadających kluczowych zabezpieczeń technicznych może być analizowane jako czyn nieuczciwej konkurencji. Wejście w życie rozporządzenia 2019/881 oraz rozpoczęcie prac nad stworzeniem unijnych ram certyfikacji technologii cyberbezpieczeństwa powoduje, że również z perspektywy prawa UE zasadne jest formułowanie pytań o odpowiedzialność producentów oraz dostawców usług za negatywne skutki incydentów bezpieczeństwa IT, oddziałujących na użytkowników indywidualnych. Do rąk Czytelników oddajemy zeszyt iKAR-a, w którym zakreślona tematyka jest podejmowana z perspektywy prawnych regulacji modelu cyberbezpieczeństwa, ale również ich konsekwencji dla stosowania przepisów z obszaru ochrony konkurencji i konsumentów.

Wprowadzeniem do tak zdefiniowanej przestrzeni badawczej jest artykuł Pawła Wajdy, w którym autor, przedstawiając analizę przepisów ustawy o krajowym systemie cyberbepieczeństwa, zastanawia się, na ile zaproponowany przez prawodawcę reżim prawny w sposób właściwy odzwierciedla oczekiwania i potrzeby rynku oraz użytkowników technologii. Rozwinięcie tych rozważań można odszukać w tekstach Stanisława Piątka oraz Tomasza Procia. Pierwszy z autorów przedstawia status przedsiębiorców telekomunikacyjnych w sprawach dotyczących cyberbezpieczeństwa z uwzględnieniem przepisów krajowych i prawa UE. Z kolei Tomasz Proć odnosi się do aktualnego zagadnienia odpowiedzialności dostawców usług cyfrowych za naruszenie zasad cyberbezpieczeństwa. Na tym tle bada kwestię ochrony użytkowników usług cyfrowych z perspektywy unijnych przepisów o ochronie danych osobowych. Czytelnika poszukującego informacji na temat uprawnień organów administracji w obszarze cyberbezpieczeństwa z pewnością zainteresuje artykuł Adama Szkurłata, w którym autor przedstawia status i kompetencje Prezesa UODO w ramach krajowego systemu cyberbezpieczeństwa.

Problem interakcji pomiędzy cyberbezpieczeństwem a prawem ochrony danych analizuje również Marcin Rojszczak. Autor koncentruje się jednak na omówieniu konsekwencji wynikających ze stosowania dyskutowanych przepisów w sektorze innowacyjnych usług finansowych (tzw. *fintech*). Innowacje finansowe to nie tylko dynamicznie rozwijający się segment usług, lecz także obszar rynku, w którym wyraźnie widać, że nowe sposoby przetwarzania danych,

a co za tym idzie także ich monetaryzacji, prowadzą do ujawnienia się nowych, wcześniej nieznanych rodzajów ryzyka, przez co stanowią również aktualne wyzwanie dla regulatorów rynku.

Z kolei Jarosław Greser podejmuje temat korzystania z wyrobów medycznych w perspektywie zagrożeń, których źródłem jest Internet oraz obecny stan prawny dotyczących badania wyrobów medycznych pod kątem cyberbezpieczeństwa. Problem bezpieczeństwa urządzeń medycznych, zwłaszcza tych używanych bezpośrednio przez pacjenta, stanowi aktualny i rzeczywisty problem z obszaru cyberbezpieczeństwa. Jednocześnie wyczerpujące odniesienie się do tego zagadnienia jest niemożliwe bez jednoczesnego uwzględnienia przepisów z zakresu ochrony danych osobowych, konsumentów i konkurencji.

Czytelników zainteresowanych regulacyjnymi aspektami funkcjonowania sieci Internet, zwłaszcza w obszarze *enforcement* zainteresuje z pewnością tekst Anny Urbanek poświęcony ochronie przed piractwem internetowym w prawie Unii Europejskiej oraz prawie federalnym Stanów Zjednoczonych. Punktem wyjścia do rozważań przedstawionych przez Autorkę jest treść rozporządzenia 2019/517 w sprawie wdrażania i funkcjonowania Domeny Najwyższego Poziomu .eu.

W kolejnym artykule Agnieszka Anusz analizuje wpływ rozporządzenia eIDAS na umowy konsumenckie z perspektywy ustawy o prawach konsumenta i ustawy o świadczeniu usług drogą elektroniczną. Na tym tle formułuje wniosek o niezbędności korelacji rozwiązań o charakterze technicznym z regulacjami w przedmiocie ochrony konsumentów.

Trzy ostatnie teksty zamieszczone w bieżącym numerze odnoszą się do problematyki wzajemnych relacji pomiędzy cyberbezpieczeństwem a normami prawa gospodarczego. W swojej analizie Katarzyna Chałubińska-Jentkiewicz podejmuje problematykę kwalifikacji prawnej oraz odpowiedzialności za dostarczane treści cyfrowe. Z kolei Łukasz Pirożek przedstawia analizę prawną partnerstwa przedsiębiorców dostarczających infrastrukturę i usługi cyfrowe oraz podmiotów publicznych w zakresie cyberbezpieczeństwa. Krzysztof Jaroszyński podejmuje natomiast problematykę wpływu nowych technologii na wykonywanie zawodu rzeczoznawcy majątkowego, a w szczególności – poszanowania zasady równej konkurencji w odniesieniu do zautomatyzowanej wyceny nieruchomości.

W bieżącym zeszycie kwartalnika zamieszczone zostały również glosy, omawiające aktualne orzeczenia z zakresu prawa ochrony konkurencji i konsumentów. Monika Bychowska dokonuje analizy wyroku SN (I NSK 58/18), dotyczącej odmowy kontraktowania na krajowym hurtowym rynku usług telewizji mobilnej świadczonych w technologii DVB-H. Z kolei Cezary Banasiński glosuje wyrok TSUE (C-532/18), w którym Trybunał dokonał wykładni prawa ochrony konsumentów w zakresie odpowiedzialności przewoźnika lotniczego za szkodę polegającą na śmierci, uszkodzeniu ciała lub rozstroju zdrowia pasażera z tytułu wypadku w rozumieniu konwencji montrealskiej.

Numer uzupełniają dwie recenzje – niedawno wydanej monografii *Public and Private Law and the Challenges of New Technologies and Digital Markets. New Technologies and Digital Markets in the light of current regulatory challenges (volume 1)* (red. nauk. E. Bani, B. Pachuca-Smulska, E. Rutkowska-Tomaszewska, Warszawa 2020) oraz *The Great Reversal – How America gave up on free markets*" (T. Philippon, Cambrige/London 2019).

Jesteśmy przekonani, że dzięki zaangażowaniu Autorów powstały ciekawe i wartościowe teksty, których lektura stanie się inspiracją dla dalszych badań w obszarze interakcji pomiędzy powstającym unijnym modelem ochrony cyberprzestrzeni a innymi obszarami prawa, w tym w szczególności ochroną konkurencji i konsumentów.

Życzymy ciekawej lektury,

Cezary Banasiński
Marcin Rojszczak