PRZEGLĄD PRAWA ROLNEGO
NR 2 (25) – 2019, 215–224

II. PRZEGLĄD PIŚMIENNICTWA

RECENZJE I NOTY RECENZYJNE

Esther Muñiz Espada, *Derecho Agroalimentario y Ciberseguridad*, Editorial Reus S.A., Madrid 2019, ss. 230.

Badanie prawa rolno-żywnościowego nie jest łatwe, choćby ze względu na zmianę regulacji prawnych, a także związaną z tym potrzebę uwzględnienia zupełnie nowych zjawisk, jak również „odświeżenia" ujęć teoretycznych. Stosowanie technologii nowej generacji i inteligentnych technik rolniczych stanowi wyzwanie nie tylko dla ustawodawcy, ale także dla nauki. Z tego względu z uznaniem należy przyjąć książkę znanej i cenionej badaczki, profesor Uniwersytetu w Valladolid, poświęconej prawu rolno-żywnościowemu w kontekście cyberbezpieczeństwa. Ten temat nie był dotąd szerzej opracowany w literaturze[1].

Jak we wstępie pisze Autorka, zastosowanie technologii nowej generacji wpływa na cały łańcuch rolno-spożywczy: produkcję, przetwórstwo i komercjalizację. Z tego względu determinuje ono zasadę ostrożności i identyfikowalności, przyczynia się do wzrostu konkurencyjności sektora, oddziałuje na środowisko, na sposoby organizacji działalności, wzajemne połączenia między obszarami wiejskimi i zarządzanie, przyczynia się do różnorodności produktów i dostaw. Jest zatem jasne, że przyszłość sektora rolno-żywnościowego zależy głównie od ekspansji nowych technologii. Jednak przy zastosowaniu w rolnictwie i przemyśle rolno-spożywczym nowych technologii mogą wystąpić zagrożenia cybernetyczne.

[1] Warto wspomnieć o artykułach: J. Martinez, *Chancen und Risiken der Digitalisierung in der Landwirtschaft – die rechtliche Dimension*, „Przegląd Prawa Rolnego" 2016, nr 2, s. 13 i n.; P. Latanzi, *L'agricoltura di fronte alla sfida della digitalizzazione. Oppopurtonità e rischi di una nuova rivoluzione*, „Rivista di Diritto Agrario" 2017, nr 4, s. 555 i n.

Pojawia się więc konieczność zapewnienia cyberbezpieczeństwa. Służy temu wieloaspektowe spojrzenie na takie problemy, jak: własność danych i ich przenoszenie, dostęp do nich, wewnętrzna operatywność danych, przekazywanie informacji i ich obieg, prywatność danych, wymiana danych za pomocą platform i ich kontrola, odpowiedzialność, trwałość innowacji w nowych modelach biznesowych i – co najważniejsze – bezpieczeństwo żywności. Jak pisze Autorka: „im bardziej polegamy na danych, tym bardziej stajemy się zależni od ich bezpieczeństwa" (s. 25).

Względy te uzasadniają strukturę pracy i wybór problemów będących przedmiotem szczegółowego opracowania właśnie z perspektywy cyberbezpieczeństwa. Autorka wychodzi od rozważań dotyczących zależności łańcucha rolno-żywnościowego od cyberbezpieczeństwa (rozdz. II), a następnie omawia regulację ochronną w zakresie bezpieczeństwa (rozdz. III). Skoro zaś przedstawia się łańcuch rolno-żywnościowy, to wypadało wyjść od charakterystyki dwóch dóbr (wody i żywności) jako „infrastruktury krytycznej" (rozdz. IV) oraz pokazać urządzenia cybernetyczne i strategię cyberbezpieczeństwa (rozdz. V). W tym kontekście Autorka prezentuje zastosowanie nowych technologii w budowaniu nowych modeli rolnych, także w przyszłej wspólnej polityce rolnej (rozdz. VI). Kolejne rozdziały dotyczą już zagadnień związanych z zapewnieniem cyberbezpieczeństwa, takich jak: wpływ nowych technologii na zasadę identyfikowalności (rozdz. VII), cyberbezpieczeństwo produktów rolnictwa ekologicznego (rozdz. VIII), cyberbezpieczeństwo a umowa doradztwa rolniczego (rozdz. IX). Całość zamykają rozważania na temat cyfryzacji towarzyszącej zmianie pokoleniowej oraz odnowy środowiska rolnego (rozdz. X).

Autorka przechodzi od charakterystyki zagadnień ogólnych do analizy wybranych kwestii szczegółowych, służących rozwinięciu argumentacji. Warto tu przytoczyć przynajmniej niektóre stwierdzenia przedstawione w pracy.

W szczególności należy zauważyć, że bezpieczeństwo cybernetyczne pełni istotną rolę w łańcuchu rolno-spożywczym choćby ze względu na wpływ mediów informatycznych i elektronicznych na bezpieczeństwo żywności. Z koniecznością gromadzenia, przechowywania i ochrony danych we współczesnej zdigitalizowanej rzeczywistości wiąże się również coraz częstsze podejmowanie prób wirtualnych oszustw, najczęściej w formie wykradania danych. Dlatego wyzwaniem dla współczesnego sektora rolnego i żywnościowego jest bezpieczne stosowanie technologii i narzędzi cyfrowych w procesie produkcji.

Aby zminimalizować zagrożenia związane z łatwością naruszania zabezpieczeń, należałoby, zdaniem Autorki, ująć w systemie prawnym działania oparte na prewencji i zintegrowanym systemie kontroli oraz ochrony. Muñiz Espada wymienia hiszpańską ustawę nr 36 z 2015 r. o bezpieczeństwie narodowym, dyrektywę 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europej-

skiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, a także hiszpańską ustawę nr 8 z 2011 r. o ustanowieniu środków na rzecz ochrony infrastruktur krytycznych. Zgodnie z postanowieniami tego ostatniego aktu prawnego w Hiszpanii opracowano pięć planów działań: Narodowy Plan Ochrony Infrastruktur Krytycznych, Sektorowe Plany Strategiczne, Plany Bezpieczeństwa Operatorów, Szczególne Plany Ochrony i Plany Wsparcia Operacyjnego.

Zastosowanie nowych technologii w rolnictwie przyczyniło się do powstania nowego zjawiska: rolnictwa precyzyjnego. Wszystkie narzędzia oparte na cyfryzacji i podłączeniu do internetu mają na celu maksymalizację efektywności produkcji rolnej przy zachowaniu kosztów na stałym poziomie albo ich zmniejszeniu. Wpisują się one również w realizację celów WPR po 2020 r., związanych także z ekologią, ochroną środowiska i zmianami klimatycznymi. Zastosowanie technologii cyfrowych pozwoli na realizację celów szczegółowych nowej WPR. W Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 2017 r. (*Przyszłość rolnictwa i produkcji żywności*) podkreślono znaczenie cyfrowej transformacji rolnictwa i obszarów wiejskich.

Prawna ochrona przed zagrożeniami cybernetycznymi powinna, zdaniem Autorki, koncentrować się głównie na infrastrukturach krytycznych, a więc systemach oraz połączonych ze sobą obiektach (w tym obiektach budowlanych, urządzeniach, instalacjach i usługach), koniecznych do zapewnienia bezpieczeństwa państwa i jego obywateli, a także sprawnego funkcjonowania organów administracji publicznej, instytucji i przedsiębiorców. Niebagatelne znaczenie ma również wykształcenie rolników, którzy są coraz lepiej przygotowani do „cyfrowego rolnictwa" (*digital farming*). Jednym z priorytetów nowej WPR będzie podejmowanie działań na rzecz szybszego włączenia młodych rolników w proces zmian generacyjnych w rolnictwie, np. przy zastosowaniu środków związanych z rolnictwem cyfrowym. We wspólnym Komunikacie Komisji Europejskiej do Parlamentu Europejskiego i Rady z 2017 r. (*Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej*) podkreślono konieczność wprowadzenia programów stażowych dla małych i średnich przedsiębiorców, opartych na zapewnieniu odpowiedniego poziomu cyberbezpieczeństwa.

Jak widać, technologie informacyjne mają coraz większe zastosowanie w rolnictwie, a ich rola będzie wzrastać. Z tego względu praca Esther Muñiz Espady jest niezwykle aktualna, porusza zagadnienia dotychczas szerzej nieopracowane, wskazuje na konieczność podejmowania określonych działań prewencyjnych i ochronnych. Zasługuje zatem na uważną lekturę.

Roman Budzinowski, Krzysztof Różański