Commission III.- CEDR Conference Poznan University –Poland- 18-21th Sept.

XXX European Congress of Agricultural Law

AGROFOOD CHAIN AND SMART FARMING

ESTHER MUÑIZ ESPADA. Universidad de Valladolid

Abstract: The agro-food law still has many challenges to overcome, however we shall bear in mind that the application of the technologies of new generation boosts its development as well as leads to the better functionality of the entire agri-food chain. Factors such as sensor technologies, satellite navigation and positioning technology, and the Internet of Things create the new future for the agrofood sectors, which requires to expand new learning skills and imposing new controls through the security. Promoting this challenge is a significant and relevant objective for the future CAP. In order to all this the question is if we have to defend a specific legislation on cibersecurity for agrofood chain, or at least specific measures of specific protocols or code of good practices for agrofood sector and even perhaps a specific legislation to prevent cyber attacks?. The agrarian field can not be addressed seriously without prior work of reorganization and legislative simplification, inserting the challenges and cybersecurity problems of the new generation technologies to agro-food production in a normative coherence that is integrated into a rationality of the agro-food sector itself. The aim of this paper is to draw the attention to the fact that without adequate levels of security during the procedure of the new technologies it will not be possible to obtain proper benefits; "*the more we depend on data, the more we depends on its security*".

Key words: Sensor technologies, satellite navigation and positioning technology, Internet of Things, smart farming, agrofood chain.

Summary: 1. New challenges for the agrofood system: new technologies and smart farming.- 2. Risks and consequences.- 3. Steps to ensure cybersecurity

regulation.- 4. How to promote the use of technologies of new generation in the future CAP.

1. The agro-food law still has many challenges to overcome, however we shall bear in mind that the application of the technologies of new generation boosts its development as well as leads to the better functionality of the entire agri-food chain[1].

Factors such as sensor technologies, satellite navigation and positioning technology, and the Internet of Things create the new future for the agrofood sectors, which requires to expand new learning skills and imposing new controls through the security

It estimates that only 25% of EU farms and farmers in the Union use above mentioned technologies which include a so called precision agriculture component in their agricultural holding (*Precision agriculture and the future of farming in Europe,* EPRS 2016, p. 35). But it is vital to mention that the future of agriculture depends mainly on the expansion of these factors.

The expansion of these means strongly conditions the models of agricultural holding, production sectors, agricultural practices, the type of professionalization of the farmer and, ultimately, the superiority and leadership of a country with respect to its geographical context. Without a doubt, competitiveness in the agricultural sector can not be understood without the application of such new generation digital technologies.

"Research and innovation are part of the foundation of progress concerning all the challenges which confront the EU's farm sector and rural areas: economic, environmental and social. The needs and contributions of rural areas should be clearly reflected on the research agenda of the European Union and the future CAP will need to enhance even more synergies with the Research and Innovation Policy in fostering innovation.

[1] This paper is framed in the research Project *Ciberseguridad en la producción agroalimentaria. Qué protocolos jurídicos de actuación*, VA049G18, de la convocatoria de subvenciones destinadas al apoyo de los grupos de investigación reconocidos de universidades públicas de Castilla y León, BOCYL 4 de junio de 2018, IP: Esther Muñiz Espada.

Technological development and digitisation make possible big leaps in resource efficiency enhancing an environment and climate smart agriculture, which reduces the environment-/climate impact of farming, increase resilience and soil health and decrease costs for farmers. However, the uptake of new technologies in farming remains below expectations and unevenly spread throughout the EU, and there is a particular need to address small and medium-sized farms' access to technology". (*Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions the future of food and farming*, COM(2017) 713 final, p. 12).

In that way, the use of technologies
-make a significant contribution to food security and safety
-has a positive impacts on the environment
-will trigger wider societal changes: will influence work practices and life conditions on farmland; and new farming business models are on the rise;

This methods promise
-to increase the quantity and quality of agricultural output while using less input (water, energy, fertilisers, pesticides...).
- to save costs,
- reduce environmental impact and produce more and better food,
-and optimise agricultural production processes (In the same meaning, it is outstanding by *Precision agriculture and the future of farming in Europe,* EPRS 2016).

2- We shall take into consideration that there are always pros and cons of that procesess. The multiplicity of data and processes increase the risks and new types of contingency which signifies the new sources of fraud and cybercrime.

The risks of attacks includes cyberterrorism or agroterrorism on agrifood production or simple attacks to the information which is incorporated into the systems used for agricultural production, with possible consequences and economic damages for the agricultural entrepreneur or for holdings or for food security; in any case, the global threat includes the area of food security.

Spain has imposed new acts on cybersecurity, but in a general way. The European Union has also a big packet regulation on cybersecurity:

- The Commission has proposed to reinforce the EU's resilience, deterrence and response to cyber-attacks by establishing a stronger European Union Cybersecurity Agency to assist Member States in dealing with cyber-attacks.

- Creating an EU-wide cybersecurity certification scheme that will increase the cybersecurity of products and services in the digital world.

- A Blueprint for how to respond quickly and a efficient way when a large scale cyber-attack strikes.

- A network of competence centres in the Member States and a European Cybersecurity Research and Competence Centre that will help develop and roll out the tools and technology needed to keep up with an ever-changing threat and make sure our defence is as strong as possible.

- A Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and measures to strengthen international cooperation on cybersecurity, (*In the European Union, Commission, State of the Union 2017, Cybersecurity, Commission scales up EU´s response to cyberattacks*).

- Regulation EU 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA -the European Union Agency for Cybersecurity- and on information and communications technology cybersecurity certification and repealing Regulation EU 526/2013 -Cybersecurity Act-.

But in our context –agrofood- the key question is: we have to defend a specific legislation on cibersecurity for agrofood chain, or at least specific measures of specific protocols or code of good practices for agrofood sector and as I said even perhaps a specific legislation to prevent cyber attacks?.

The problem is serious because it affects to public health, the economy, the environment, the security of States, the agri-food industry and holdings in this sector. In that way, the more essential is to guarantee the security food because "*the more we depend on data, the more we depends on its security*" *(Cybersecurity in the Agrifood sector, Securing data as crucial asset for agricultura, Capgemini Consulting, Wageningen UR).*

The current challenge of agricultural law is the safe application to the agricultural and agri-food environment of the digital technologies and tools for production, since these techniques are especially threatened by vulnerability and by the ease of breaking their security.

The Global Risks Report 2019 warns: "Technology continues to play a profound role in shaping the global risks landscape for individuals, governments and businesses. In the GRPS, "massive data fraud and theft" was ranked the number four global risk by likelihood overa 10-year horizon, with "cyber-attacks" at number five. This sustains a pattern recorded last year, with cyber-risks consolidating their position alongside environmental risks in the high-impact, high-likelihood quadrant of the Global Risks Landscape …. A large majority of respondents expected increased risks in 2019 of cyber-attacks leading to theft of money and data (82%) and disruption of operations (80%)", p. 16. "Concerns about data fraud and cyber-attacks were prominent again in the GRPS, which also highlighted a number of other technological vulnerabilities: around two-thirds of respondents expect the risks associated with fake news and identity theft to increase in 2019, while three-fifths said the same about loss of privacy to companies and governments. There were further massive data breaches in 2018, new hardware weaknesses were revealed, and research pointed to the potential uses of artificial intelligence to engineer more potent cyber-attacks. Last year also provided further evidence that cyber-attacks pose risks to critical infrastructure, prompting countries to strengthen their screening of cross-border partnerships on national security grounds".

3- The Union has already taken important steps to ensure cybersecurity and to increase trust in digital technologies. In 2013, the Cybersecurity Strategy of the European Union was adopted to guide the Union's policy response to cyber threats and risks. In an effort to better protect citizens online, the Union's first legal act in the field of cybersecurity was adopted in 2016 in the form of Directive EU 2016/1148 of the European Parliament and of the Council. Directive EU 2016/1148 put in place requirements concerning national capabilities in the field

of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between Member States, and introduced obligations concerning security measures and incident notifications across sectors which are vital for the economy and society, such as energy, transport, drinking water supply and distribution, banking, financial market infrastructures, healthcare, digital infrastructure as well as key digital service providers -search engines, cloud computing services and online marketplaces-, (in *Regulation EU 2019/881 of the European parliament and of the Council of 17 April 2019 on the European Union Agency for Cybersecurity and on information and communications technology cybersecurity certification -Cybersecurity Act)-*.

With a view to ensuring the proper functioning of the internal market while aiming to achieve a high level of cybersecurity, cyber resilience and trust within the Union, this Regulation lays down:(a) objectives, tasks and organisational matters relating to ENISA (the European Union Agency for Cybersecurity); and(b) a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity for ICT products, ICT services and ICT processes in the Union, as well as for the purpose of avoiding the fragmentation of the internal market with regard to cybersecurity certification schemes in the Union.The framework referred to in point (b) of the first subparagraph applies without prejudice to specific provisions in other Union legal acts regarding voluntary or mandatory certification. 2. This Regulation is without prejudice to the competences of the Member States regarding activities concerning public security, defence, national security and the activities of the State in areas of criminal law. (art. 1).

1. ENISA shall be a centre of expertise on cybersecurity by virtue of its independence, the scientific and technical quality of the advice and assistance it delivers, the information it provides, the transparency of its operating procedures, the methods of operation, and its diligence in carrying out its tasks.

2. ENISA shall assist the Union institutions, bodies, offices and agencies, as well as Member States, in developing and implementing Union policies related to cybersecurity, including sectoral policies on cybersecurity.

3. ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member

States and public and private stakeholders, to increase the protection of their network and information systems, to develop and improve cyber resilience and response capacities, and to develop skills and competencies in the field of cybersecurity.

4. ENISA shall promote cooperation, including information sharing and coordination at Union level, among Member States, Union institutions, bodies, offices and agencies, and relevant private and public stakeholders on matters related to cybersecurity.

5. ENISA shall contribute to increasing cybersecurity capabilities at Union level in order to support the actions of Member States in preventing and responding to cyber threats, in particular in the event of cross-border incidents.

6. ENISA shall promote the use of European cybersecurity certification, with a view to avoiding the fragmentation of the internal market. ENISA shall contribute to the establishment and maintenance of a European cybersecurity certification framework in accordance with Title III of this Regulation, with a view to increasing the transparency of the cybersecurity of ICT products, ICT services and ICT processes, thereby strengthening trust in the digital internal market and its competitiveness.

7. ENISA shall promote a high level of cybersecurity awareness, including cyber-hygiene and cyber-literacy among citizens, organisations and businesses (art. 4 –objectives-).

In short, the objectives are:

-to increase the capacities and preparedness of Member States and companies;

- to improve cooperation and coordination between the Member States and EU institutions, bodies and agencies;

-to increase capacities at the EU level to complement the action of the Member States, in particular in the case of cross-border cybercrisis;

-to Increase the awareness of citizens and businesses about issues related to cybersecurity;

- to increase the transparency of the cybersecurity guarantee

In that way,

ENISA should actively support actions taken by Member States to comply with their obligations under Directive (EU) 2016/1148 and therefore should not supersede them.

ENISA should also assist with the development and updating of strategies on the security of network and information systems at Union level and, upon request, at Member State level, in particular on cybersecurity, and should promote the dissemination of such strategies and follow the progress of their implementation.

ENISA should support Member States in the field of cybersecurity awareness-raising and education by facilitating closer coordination and the exchange of best practices between Member States.

ENISA should assist providing expertise, advice and by facilitating the exchange of best practices, regarding risks and incidents.

ENISA should stimulate cooperation between the public and private sector and within the private sector, in particular to support the protection of the critical infrastructures, (*Whereas 25-31 Act cibersecurity*).

4.- The future post-2020 CAP promises significant changes under increasingly stringent policies from the environmental point of view, quality, and greater competitiveness of farms, which is exactly connected to this new type of agriculture that goes through the promotion or the role of digitalization. Its objectives are to improve market orientation and increase competitiveness, in particular, with greater emphasis on research, technology and digitalization.

The question is how to address the challenge, the principal question is: it is necessary a specific regulation to guarantee the cybersecurity in the agrofood chain or it is enough the general legislation?, how to promote exactly the precision agriculture?, because it has pros and cons, it has consequences in the high production and in the reduction of the resources but it reduce also the emploees, and how to protect the owner of the big data generate by the news technologies or how to share the data between farmers?; to control the traceability in a food

supply chain is another componen in this debate when we use technologies of new generation.

The agrarian field can not be addressed seriously without prior work of reorganization and legislative simplification, inserting the challenges and cybersecurity problems of the new generation technologies to agro-food production in a normative coherence that is integrated into a rationality of the agro-food sector itself.

BIBLIOGRAPHY

AYERBE, A., "La ciberseguridad de la industria 4.0: un medio para la continuidad del negocio", *Economía industrial*, nº 410, 2018.

BARATTA MARTINEZ, R., "Gobierno de la ciberseguridad", *Economía industrial*, nº 410, 2018.

BENNETT, J.M., "Agricultural Big Data: Utilisation to Discover the Unknown and Instigate Practice Change", *Farm Policy Journal*, 2015.

BRONSON, K., KNEZEVIC, I., "Big data in food and agricultura", *Big Data & Society*, 2016.

BUSNELLI, F.-SIRSI, E., "Techonological innovation in agricultura and legal choices (from disparity to diversity)", *Riv. di Diritto agrario*, 2009.

CANFORA, I., "Il principio di precauzione nella gobernance della sicurezza alimentare: rapporti fonti in un sistema multilivello", *Riv. di Diritto agrario*, 2017.

- "Informazioni a tutela della salute e conformazione del contenuto negoziale tra Diritto europeo e Diritto nazionali", *Riv. di Diritto agrario*, 2014.

DABBENE, F.-GAY, P.,-TORTIA, C., "Traceability issues in food supply chain management: A review", *Biosystems engineering,* 2014.

DE MAURO, A., GRECO, M., GRIMALDI, M., "A formal definition of Big Data based on its essential features", *Library Review*, 2016.

ERICKSON, B., WIDMAR, D.A., "Precision Agricultural Services Dealership Survey Results", West Lafayette, 2015, Purdue University. http://agri

business.purdue.edu/files/resources/2015–crop–life–purdue–precision–dealer–survey.pdf.

FARKAS, TJ., "Data Created by the Internet of Things: the New Gold witout Ownership?", *Prop. Inmaterial*, 5, 2017.

FEATHERSTONE, A.M. , "The Farm Economy: Future Research and Education Priorities", *Applied Economic Perspectives and Policy* 40, 1, 2018.

MUÑIZ ESPADA, E., *Derecho agroalimentario y ciberseguridad*, Reus, Madrid, 2019.

ORTIZ PRADILLO, J. C., *Problemas procesales de la ciberdelincuencia*, Madrid, ed. Colex, 2013.

POPPE, K, WOLFERT, S., VERDOUW, C., VERWAART, T., "Information and Communication Technology as a Driver for Change in Agri-food Chains", *EuroChoices* vol 12. Nr. 1, 1 2013; POPPE, K., WOLFERT, S., VERDOUW, C., RENWICK, A., "A European perspective on the economics of big data", *Farm Policy Journal*, Vol. 12, n. 1, 2015.

PORTER, M.E., HEPPELMANN, J.E., "How Smart, Connected Products Are Transforming Competition", *Harvard Business Review*, 2014.

RIBARICS, P., "Big data and its impact on agricultura", *Ecocycles*, 2016.