Cybersecurity and Agricultural-food supply chain

ESTHER MUÑIZ ESPADA. Universidad de Valladolid
Agri-food law still has many challenges to overcome, one of which is the application of the technologies of new generation. We should bear in mind that the application of these technologies 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 agri-food sectors, which requires to expand new learning skills and imposing new controls through the security.

It is estimated 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 cannot be understood without the application of such new generation digital technologies.
The use of technologies
- makes a significant contribution to food security and safety
- has 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.

These 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).
• We should take into consideration that there are always pros and cons of these processes. 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 on 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).


But in our context – agrifood – the key question is: we have to defend a specific legislation on cybersecurity for the agrifood chain, or at least specific measures or specific protocols or code of good practices for agrifood sector?
• The problem is serious because it affects: public health, the economy, the environment, the security of States, the agri-food industry and holdings in this sector. In that way, the most essential is to guarantee the security of food because “the more we depend on data, the more we depend on its security”

(Cybersecurity in the Agrifood sector, Securing data as crucial asset for agricultura, Capgemini Consulting, Wageningen UR).
• 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 of 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 questions are:
  - is a specific regulation necessary to guarantee cybersecurity in the agrifood chain or
  - is the general legislation enough?,
  - how to promote exactly precision agriculture?, because it has pros and cons, it has consequences in the high production and in the reduction of the resources but it reduces also the number of employees,
  - how to protect the owner of the big data generated by the news technologies or how to share the data between farmers?;
  - and to control the traceability in a food supply chain is another component in this debate.

• To sum up or to finish: 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 agri-food sector itself.