Legal Risks and Chances of Automation in Agriculture

Is EU regulation stifling or promoting innovation?

RA Florian Mörth, RA Dr. Julia Pfeil, Dentons Europe LLP, Frankfurt

Abstract

Legal frameworks may form enablers of, or barriers to, adoption of new automation technologies in agriculture. This paper examines regulatory structures, or rather lack of them, for new automation technologies in the EU – as a small case study illustrating selected issues for manufacturers and component suppliers. It also examines how the law may provide elements of an answer to these legal issues and how solutions can be developed to enable smooth operations of new degrees of automation in agriculture.

1. Introduction

New automation technologies, driven by data and incorporating emerging techniques – such as Internet of Things (IoT) and Artificial Intelligence (AI) – are setting the grounds for the future of agriculture [1]. By fostering a healthy environment, economic profitability, and social and economic equity, new degrees of automation have the potential to transform and empower the agricultural sector [2]. Simultaneously, automation presents unprecedented challenges from a technical, but also from an EU legal standpoint. Relevant stakeholders in agriculture will likely only embrace new automation technologies, corresponding processes will only be efficient and investments will only be protected, if legal risks are addressed, thus ensuring mutual benefit. Public regulatory bodies in the EU expect compliance in particular from manufacturers and component suppliers of new agricultural automation systems. Concurrently, the legal implications surrounding new degrees of agricultural automation (such as civil product liability or product safety obligations) are partly unclear and raise complex legal questions; namely because of the diversity of potentially applicable or missing regulatory regimes, sparse case law and in parts no substantial, in depth, academic or practitioner analysis on the requirements associated with the regulation of new automation technologies in agriculture.

In view of the foregoing, this paper focuses on selected legal issues of new agricultural automation systems that arise in the EU regulatory context, with emphasis on product liability in general and, more specifically, regarding AI-enabled autonomous systems. There-
by the focus lies on implications for manufacturers and component suppliers. It also examines how the law may provide elements of an answer to these legal issues and how solutions can be developed to enable smooth operations of new degrees of automation in agriculture. In the broader context of new agricultural automation systems, there are, in addition, numerous other legal issues arising from different laws – governing data privacy and ownership, anti-trust or infrastructure security – which require analysis beyond this paper.

2. Product Liability
Rapid changes in agricultural automation technologies and the ways in which food is produced open potential for new product defects – with serious consequences. Particularly IoT-based automation in agriculture may integrate multiple cross-domain data streams (e.g. meteorological data, soil condition data etc.) providing a complete semantic processing pipeline for data-driven automation in agriculture [3]. The seamless interoperability among sensors, services, processes, operations, farmers and other relevant parties, including online information sources and linked open datasets and streams may lead to a growing potential for product defects. Agricultural automation also increasingly depends on networked systems. Reliance on networked systems has brought the security of software systems under considerable scrutiny. Built on an extended notion of a “defect”, security and reliability have become important attributes of complex software systems – especially in the context of cyberattacks. Defective products not only pose a serious safety risk to the public but can also cause significant financial damage to the companies responsible. Even a short-duration interruption by a cyber-intrusion of a highly time-sensitive task such as harvest could cause significant economic losses [4]. All of the above issues are only compounded with an ever increasing degree of automation in agriculture.

It is therefore crucial for manufacturers and component suppliers to identify risks associated with civil product liability laws that may arise from potential product defects, such as cybersecurity vulnerabilities. As concisely noted by security expert Bruce Schneier, “liability changes everything” [5]. Since developing and maintaining robust automation systems in agriculture entails high costs, civil legal liability intends to create incentives in order to motivate the industry to work towards a higher level of safety and security [6] – at least from a policy standpoint. But manufacturers and component suppliers currently face a great deal of uncertainty when assessing the risk of civil product liability that may arise from unintended defects. This issue is compounded by an evolving and fragmented as well as absent and unclear legal landscape.
The civil product liability regime in the EU primarily builds on the Product Liability Directive 85/374/EEC – adopted in 1985 – which has been transposed into national law by Member States. With regard to B2C, the Directive imposes strict tort liability on producers of defective products. Alongside this, general principles of product tort (and contract law) may apply in each Member State on a B2C and B2B level. At its core, the Directive still intends to regulate the defective implementation of “analog” technologies [7]. Therefore, difficulties arise in respect of the application of the Directive in certain technological contexts.

Taking for instance complex control algorithms deployed with the embedded software of new agricultural automation systems: It would be difficult to assess the civil product liability exposure of the responsible manufacturer or component supplier for claims for personal injury and property damage caused to third parties due to product defects. Under the Directive software is also not considered a product – only if it is stored on a physical storage medium (e.g. hard drives) [8]. Furthermore, it is particularly unclear how the term “product defect” will be interpreted with respect to new automation technologies in agriculture. Under Article 6 of the Directive, a product is defective “when it does not provide the safety which a person is entitled to expect, taking all circumstances into account, […]”. IoT devices (e.g. sensors) that support higher degrees of automation can be notoriously problematic with regard to defects. Thus, the complex question arises what level of safety one is generally “entitled to expect” from new automation technologies in agriculture. Such expectations of safety may also further vary depending on the specific market. According to German courts, prevention of possible “misuses of a product” – most notably cyber-intrusions – are generally not to be expected [9]. To this end it appears that respective manufacturers and component suppliers of new automation technologies are effectively insulated from liability for product defects where such liability arises in a situation that falls outside the scope of the Product Liability Directive.

Nevertheless, manufacturers and component suppliers may be subjected to national tort regimes in other respects. At least in Germany, manufacturers and component suppliers have to principally meet a duty of care after their product has been placed on the market. “Producers” – including software developers – are obligated to monitor their products for previously undetected security vulnerabilities as well as other defects and, if necessary, take measures to avert emanating risks [10]. However, in this respect, difficult legal questions arise from new agricultural automation technologies in Germany. First, it is unclear, if under this duty of care monitoring measures have to be technically integrated into the product, as product-integrated monitoring solutions may be available on the market [11]. In case of monitored defects, it is also unclear if settled German case law applies. The question arises, if manufacturers and component suppliers are obligated to update/patch their systems by
available remote access. Often development methodologies (rightly) do not focus on the quality or security of a product but rather on functionality and time-to-market [12]. According to the Federal Court of Justice (Bundesgerichtshof) [13] manufacturers and component suppliers are – at least for the moment – only required to warn operators about any defects detected if this is sufficient to avert risks. Be it as it may, unlike in the available case law, where product updates required cost-intensive product recalls, remote updating processes are principally more cost-efficient; it is often only a matter of a mouse-click to update software accordingly. Another issue to be considered is the standard of care which ought to apply to new agricultural automation systems in the future. Standards may evolve with changes and developments in the degrees of automation. This raises the issue of software updates and patches in agricultural automation in a much more general way. Contrary to a (potential) duty of care, software updates/patches may not always be available. Agricultural automation systems may be designed without the ability to accommodate firmware or software updates, thus creating factual constraints.

To that end the Regulation on Software Updates and Software Update Management Systems by the UNECE’s World Forum for Harmonization of Vehicle Regulations (WP.29) – which will be implemented into EU law before 2021 – is relevant. The UN Regulation applies to agricultural vehicles permitting software updates (categories R, S, T). Unfortunately, at this moment, it is unclear how the framework will affect the civil product liability regime in the EU. The new regime will require the agricultural vehicle sector to put in place software updating processes, such as for identifying vehicle targets and verifying their compatibility with an update or assessing if a software update affects the type approval.

It is also frequently forgotten that EU product safety rules and regulations set forth very specific and strict technical standards in relation to new automation systems – especially in agriculture. These standards apply not only to OEMs and system integrators, but also to component suppliers and finishers who see a high market potential for new technologies, such as embedded software systems, IoT networking or driver-assistance systems. Violations of EU product safety rules and regulations may lead, among other consequences, to civil product liability, product recalls and fines. EU rules on product safety for new agricultural automation systems are generally defined in the General Product Safety Directive 2001/95/EC. In addition, there are a series of regulations that are particularly relevant to new automation technologies in agriculture. The safety requirements for machines are specifically regulated in Directive 2006/42/EC. Lex specialis is the Regulation 167/2012/EU on the approval and market surveillance of agricultural and forestry vehicles. Furthermore, the Radio Equipment Directive 2014/53/EU, Low Voltage Directive 2014/35/EU or the Electromagnetic
Compatibility Directive 2014/30/EU may apply. Concerning agricultural automation systems, the related norm EN ISO 18497:2018 on principles for design of agricultural machinery and tractors regarding safety of highly automated agricultural machines is of considerable importance. It is to be noted that the rules and regulations listed above do not yet, contain any AI-specific requirements.

Finally, it is worth noting that EU product safety law is about to enter a new era of enforcement. Principally, as of 16 July 2021, the new EU Market Surveillance Regulation 2019/1020/EU will apply. The Regulation strengthens controls on harmonized products sold in the EU by introducing a number of key changes, such as significant expansion of market surveillance powers (including access to software embedded in products, details of the supply chain/distribution channel and quantities of products on the market, unannounced on-site inspections as well as reverse engineering and access rights).

In addition, Member States such as Germany are considering expanding (cyber-) security oversight of IT systems that are also relevant to automation technologies in agriculture. The Federal Ministry of the Interior is proposing extensive and far reaching changes to the Act on the Federal Office for Information Security [14]. Among other regulations, the bill authorizes the competent authority (BSI) to audit all available IT products on the German market for compliance with (cyber-) security standards – even without a particular reason. This includes products "intended for provision", i.e. products still in development. The proposed amendment to the Act could see fines of up to EUR 20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher – at present, the Act stipulates a maximum penalty of merely EUR 100,000 [15]. Respectively, manufacturers and component suppliers should consider monitoring how legislatures shape new product security provisions applicable to their product.

In light of the above, product-related risk is one of the biggest perils facing manufacturers and component suppliers of complex automation systems, with recall exposures having increased significantly over the past decade. As such, manufacturers of new automation technologies in agriculture and their component suppliers should consider relevant adjustments to their quality control systems to manage product liability risks. This may include suitable quality assurance agreements with contractual partners, determination of appropriate criteria for the delimitation of risk areas or the allocation of specific interests in a shared production environment. In some cases, simply updating or developing new quality management manuals, liability guidelines, product descriptions and instructions for use will suffice to manage risk exposure. In addition, proactively implementing monitoring technology in new automation systems to prevent and drive future recall risks (e.g. by remote maintenance and up-
dating functions) can be considered as part of a product life cycle management (PLM) framework – if they are not mandatory. In limited cases, where adjustments to quality control systems do not minimize product liability risks, an insurance for new automation technologies or adjustments to a product recall management system may mitigate liability. Understanding the root cause of the technical problem is essential in the event of a product recall. Complex automation systems in agriculture may consist of numerous different components of software and hardware – from different suppliers or joint manufacturers. Therefore, to identify product defects in a timely and cost efficient manner, technical documentation and the traceability of components (e.g. by way of product-embedded monitoring systems) should increase in relation to the complexity of the automation system. This may also include storage of accident data in order to comprehensively reconstruct an accident. Such proactive approaches may prevent product recalls from the outset.

In light of civil product liability and other repercussions, rightfully hardening any system, i.e. securing it by reducing its surface of vulnerability (e.g. by encryption) may lead to unintended and paradox consequences in the supply chain. New automation technologies in agriculture may cross national borders. With regard to hardened systems, this may entail export licensing requirements under relevant export control regulations. Products that are, for example, designed or modified to use certain cryptographic functions are governed by encryption export controls (especially in the US and the EU) [16]. That is because most countries, to varying degrees, regulate encryption as a so-called dual-use item, having both civilian and military applications. Such elements should be taken into account at the development stage of the product life cycle by manufacturers and component suppliers as they may negatively impact the marketability of new automation technology in agriculture.

3. Focus: AI-enabled Autonomous Agricultural Systems

Further to the above, many other legal issues surrounding civil product liability arise within the context of automated agricultural systems, especially with respect to highly or fully autonomous systems. This is most notably the case when “intelligent” technologies are leveraged, such as AI (e.g. Machine Learning, Computer Vision or Context-Aware Computing). Intelligent and autonomous systems (e.g. AI-enabled harvesting and crop sprayer robots) are able to maximize yield and at the same time safeguard and make more efficient use of natural resources [17]. But as things currently stand, such benefits cannot be realized fully by European agricultural market participants. This is, to a significant extent, due to an absent, fragmented and unclear regulatory framework, which fails to address and resolve issues in relation to potential risks emerging as a consequence of the use of autonomous technolo-
gies. The existing regulatory frameworks in the EU – especially the civil product liability regime – seem particularly incapable of managing the risks associated with AI-enabled autonomous systems in agriculture. Current ex ante regulation is unsuited, because AI solutions – not just in agriculture – tend to be discrete (components of an AI system may operate without conscious coordination), diffuse (allocation of responsibilities between different parties for autonomous decisions is unclear) and not transparent (AI algorithms may be “black boxes” to outside observers but even also to their creators) [18]. Legal doctrine is also generally focused on specific human conduct and not autonomous decision making. Moreover, regulation at any stage is complicated by the difficulty in defining what, exactly, “artificial intelligence” means.

In the absence of a clear picture on tort liability, current product law is especially not able to meet the demands of deploying autonomous farming systems. AI is an emerging technology that is prone to failures. With its actions AI may cause damages for one reason or another; and thus issues of compensation will have to be addressed. One of the main problems regarding tort liability for AI technology in agriculture is that EU product law is not able to allocate liability in the context of diffuse AI systems. Without a legal framework, it is inherently unclear who “controls” an intelligent and autonomous system and thus who should be held liable in tort: The person primarily deciding on and benefitting from the use of the system (operator) or the person continuously defining the features of the technology and providing backend support (e.g. manufacturer/component supplier)? Similarly, the issues associated with foreseeability and causation are outside of the scope of EU product law. If, for example, very complex AI algorithms use multiple data streams from several data providers/sources and a defective data set and/or a defective algorithm causes damage, it may be very hard to prove (to the contrary) the existence of an element of liability beyond what can be reasonably expected [19]. In view of this, the modification of the premises of fault-based liability (especially the distribution of the burden of proving fault) or establishing liability that is independent of fault (usually called strict liability or risk-based liability) are being discussed as possible legal solutions [20] – if the European regulator does not address these issues.

In February 2020, the European Commission published its report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics [21]. Alongside this report, a white paper on a European approach to artificial intelligence was published [22]. The Commission proposes updating the existing product law framework to ensure, among other things, that compensation is always available for damage caused by products that are defective because of software. The EU Commission is also considering whether it should alter the burdens of proof on plaintiffs – which are currently required by Member State liability
rules for AI systems. In addition, the Commission also acknowledges that the complexity of IoT/AI products contributes to difficulties in establishing what components caused a malfunction, which may make it difficult to prove liability in cases involving such products. In light of possible changes, manufacturers and component suppliers should consider participating with industry groups and government agencies to develop ethical guidelines and industry standards that reflect the benefits, risks, and limitations of agricultural automation systems with AI.

To harness the opportunities of autonomous technology in agriculture and to intelligently manage the potential risks emanating from this new future, relevant parties should consider the often unappreciated legal protections that are available, such as contractual warranties and indemnities. However, there are no legal blueprints. Only a multifaceted, case-by-case legal approach may help to bridge the current gap in the regulatory framework. An adequate legal risk management framework may include, for example, contractual limitations of liability, adequate operating instructions or establishing policies for handling liability risk in the development stage of the product lifecycle (e.g. accountability, explanation, data governance, audibility, validation and testing of AI technology). The latter may especially be important in the context of regulatory compliance and as a defense of civil liability before a court of law.

4. Conclusion

The EU product regulatory regime which applies to manufacturing and development of new automation technologies in agriculture appears to be complicated, fragmented and partly outdated. However, an essential aspect of this regime is that parties have different rights and obligations under different laws which may make it possible to allocate liabilities. The law also allows defenses in certain cases which are particularly specific and relevant for promoting developments in technology. Even more compellingly, where permitted by law, parties may re-allocate legal liabilities specific to new automation technologies in agriculture.

In case of outstanding issues such as the legal status of autonomous agricultural systems tangible legal solutions may be developed in certain cases. In the corresponding process, it is essential to take a holistic and case-by-case view of legal risks by integrating the operational concerns of an agricultural automation venture with legal concepts, such as dynamic contractual arrangements or risk-based analysis. Where legal barriers cannot be overcome, legislative action may be warranted to address and distribute legal risks adequately. The agricultural automation sector would be ill advised to go along with such a change without drawing attention to legitimate concerns, such as technical neutrality of the regulatory system, i.e. the freedom of individuals and organizations to choose the most appropriate and
suitable technology for their needs [23]. Lastly, there are numerous other legal issues arising in the broader context of new agricultural automation systems (e.g. from data governance and data privacy law) which require analysis beyond this paper.


[16] Cf. e.g. Annex I, Category 5 Telecommunications and “Information Security” dual-use Regulation 428/2009/EC.


[23] Since 2011, technology neutrality has been recognized as a key principle for internet policy (OECD, 2011).