Six Questions on Data and Privacy to…

Roeland de Bruin

April 8, 2022 Roeland de Bruin received his doctoral from Utrecht University on the topic of autonomous vehicles and the European regulation thereof. Recently his dissertation 'Regulating Innovation of Autonomous Vehicles: Improving Liability & Privacy in Europe' was published. We spoke with him about his research.

Question 1) What has been the starting point for your research and therefore your dissertation?

Around ten years ago, Professor Madeleine de Cock Buning asked me to represent our institute at a robotics-conference in Västerås, Sweden, to talk about the legal issues that could surround the development and deployment of several types of robots in society. The congress hall was chock-full of robot- and computer scientists, developers, and manufacturers of robot-technology (and one pitiful lawyer…), who were adamant that law in general formed a hurdle for innovation. Having my academic roots in both law and computer science – and being addicted to new technology, I was triggered by their statements – and took them home to our institute. From that moment onwards, I participated in research proposals, many other conferences and even had the opportunity to advise the European Parliament regarding the interfaces between regulation, robotics- and AI-innovation, and the societal acceptance of innovation results. Meanwhile, the fundamentals of my dissertations were laid…

Question 2) What role do data and privacy have within this research?

A very significant role. My research question regards the interrelations between liability- and privacy regulation and innovation in the field of autonomous vehicles (AV), so at least a third of my research is dedicated to privacy protection of drivers, passengers and those who encounter self-driving cars. Large-scale data processing is necessary for the development of AV-technology, and to operate the cars on the road. Also, data-storage and analysis are often necessary to determine the cause of AV-related accidents and thus liability of one or more parties to remunerate damages. Many of these data are personal data in the sense of the European privacy rules, and the processing thereof needs to be in conformity with the privacy- and data protection rules.

> "It is important that those to whom the privacy rules apply are involved in the regulatory process."

Question 3) How do you think privacy can be maximized in this case?

One of my recommendations is that the liability frameworks should be less dependent on the processing of personal data, i.e. that the currently applicable fault-based liability rules incorporated in the product- and traffic liability frameworks, are converted into risk-based rules. That would significantly decrease the need for the processing of personal data of the operators, passengers and victims of AVs that are involved in an accident. Furthermore, it should become easier to draft and adopt sector-specific codes of conduct, and certification mechanisms for AV-developers and deployers regarding data protection. As it stands, it is often uneasy for AV-innovators to understand what the GDPR-rules implicate for them, and to comply with these in general – resulting in high risks of under-protection of citizens' rights, which implicate at the same time high DPA-enforcement and liability risks for innovators. For the sake of legal certainty for innovators, subsequent compliance with those rules and thus the protection of the privacy for AV-consumers, it should be encouraged that more specific rules are drafted that are applicable throughout the AV-innovation chain.

Question 4) In the book, the term "regulatory frameworks" appears frequently. Why didn't you just focus on the GDPR, as it aims to provide an overarching and Union-wide set of data protection rules?

The GDPR is part of a broader ecosystem of rules, to which I call a "regulatory framework" in my book. With that term, I refer to all the rules that are applicable to a certain topic. Regarding "personal data protection" those include for instance the rules that are comprised within the EU fundamental rights catalog, the General Data Protection Regulation (and other regulations/directives), and the national rules regarding data privacy, but also guidelines and regulations of the data protection authorities, sector-specific rules and case law of the national and European courts. Albeit I do suggest to make some alterations in the GDPR, it may be equally important to focus the regulatory attention to other parts

“Both the liability and the privacy frameworks would need to be improved.”

of the regulatory framework, for instance codes of conduct and certification mechanisms.

Question 5) Can you tell us a bit more about the “bottom-up” approach you refer to in your dissertation?

It is important that those to whom the (privacy) rules apply, are involved in the regulatory process. To maximise legal certainty, and subsequent compliance with such rules, it is important that stakeholders in the AV-sector are invited to help drafting the privacy rules that apply to them and their products and services, which are subsequently endorsed and adopted by the state-regulator (the EU institutions and the delegated regulators, including for instance the European Data Protection Board and the local data protection authorities). Although the GDPR contains mechanisms to this end, for instance in the form of codes-of-conduct and certification mechanisms, it appears that these do not work well at the moment, since there are only a handful of such bottom-up initiatives that are (being) adopted currently. It is observed that the approaches to bottom-up regulation as enshrined in the GDPR are too cumbersome for the stakeholders to participate in, and that the data protection authorities appear to be very strict in their assessment of the sector-specific rules that would result from these bottom-up regulatory processes.

Question 6) You make a number of recommendations to the European legislature to achieve the best outcome. Can you provide us with a small glimpse into such a recommendation?

Both the liability and the privacy frameworks would need to be improved, to provide better conditions for innovation and acceptance of AVs in the EU. Regarding the privacy frameworks, I think it is important to improve legal certainty for innovators – using a bottom-up approach as much as possible, inter alia regarding the:

- lawfulness of the processing of (special category) data through AVs and the accident prevention and registration systems;
- the criteria for conducting data privacy impact assessments and the qualification of potential “high risks” that could remain for data subjects;
- the technical and organisational measures to be taken by AV-developers; and as to
- when the privacy-by-design and privacy-by-default-obligations can be deemed to be fulfilled.

Furthermore, it should be investigated how decentralized storage of AV-data (for accident prevention and registration purposes) for instance through blockchain-technology could be brought in compliance with the GDPR. Also, a solution is necessary for the currently problematic data-transfers between the EU and the US after the Schrems II-decision of the Court of Justice of the European Union. To conclude, I recommend to introduce (further) procedural aids for victims of (alleged) GDPR-violations in the form of rebuttable presumptions of a norm-violation and causality when a controller (or processor) breached a GDPR-obligation, and to clarify on a European level, which immaterial damages would qualify for remuneration under the GDPR’s liability provisions.

About the author
Roeland de Bruin combines law and technology. In his work as Assistant Professor at Utrecht University, he investigates the interfaces between regulation and technological innovation, whereby he mainly focuses on privacy, liability and intellectual property law. As an attorney-at-law at KienhuisHoving NV, he mainly works for clients in the AI and tech-sector, and advises public institutions who address the challenges and opportunities that innovative technology may pose.

News

Cyber posture: Council approves conclusions

Cyberspace has become a place for geopolitical competition and therefore, with the EU, can be able to respond to cyberattacks. In light of this, The Council approved conclusions on developing the Union’s cyber posture. The purpose is to show that the European Union is committed to seeking long-term solutions to threat actors to the open and secure European cyberspace.

https://www.consilium.europa.eu/nl/press/press-releases/2022/05/23/cyber-posture-council-approves-conclusions/

Highest fine ever for Dutch Tax Authority

The Dutch Data Protection Authority has imposed a hefty fine on the Tax Authorities, namely 3.7 million euros. The reason for this is that this government service has illegally processed personal data in the Fraud Signaling Facility (FSV) for many years. As a result, many people were wrongly on without reason. This fine is the highest fine the DPA has ever given.

https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-zwarte-lijst-fsv

Trend alert: technology trends in banking and investment

Gartner identifies three upcoming trends that are bound to gain traction in 2022. First, banks will start to apply generative AI more, specifically in growth areas. Second, more advanced forms of autonomic systems will emerge. Third, Gartner estimates that by the year 2025, roughly 60% of large organizations will use one or more privacy-enhancing computation.

https://www.gartner.com/en/newsroom/press-releases/2022-05-24-gartner-identifies-three-technology-trends-gaining-tr