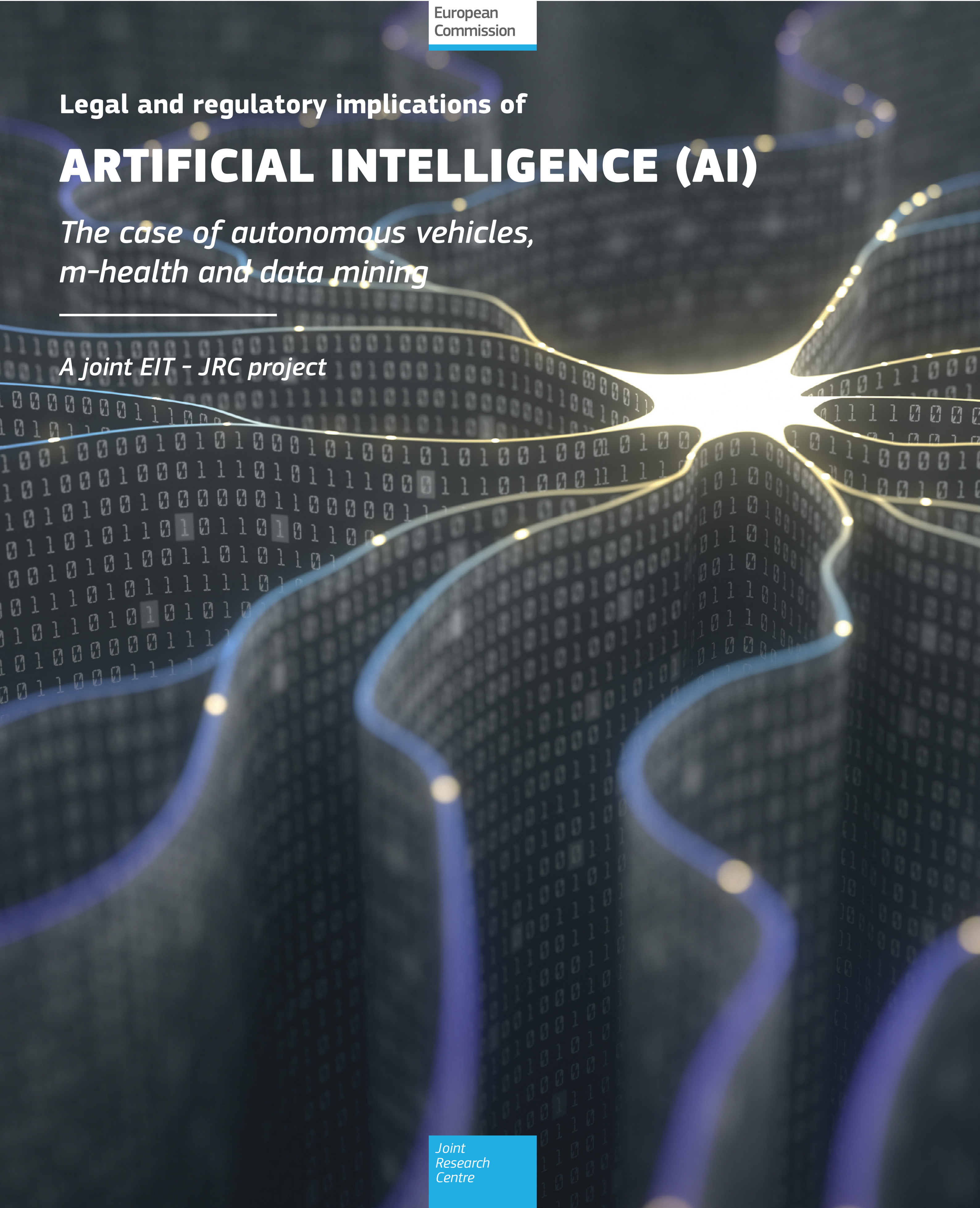
European Commission



Legal and regulatory implications of

ARTIFICIAL INTELLIGENCE (AI)

The case of autonomous vehicles, m-health and data mining

A joint EIT - JRC project

Joint Research Centre

This publication is a Conference and Workshop report by the Joint Research Centre (JRC), the European Commis-sion's science and knowledge service. It aims to provide evidence-based scientific support to the European poli-cymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

EU Science Hub
https://ec.europa.eu/jrc

JRC116235

PDF ISBN 978-92-76-02040-0 doi:10.2760/527052

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: Holder C. (ed.), Iglesias, M. (ed.), Triaille J.-P., Van Gysegnem J.-M., *Legal and regulatory implications of Artificial Intelligence. The case of autonomous vehicles, m-health and data mining*, Publication Office, Luxembourg, 2019, ISBN 978-92-76-02040-0, doi:10.2760/527052, JRC116235.

TABLE OF CONTENTS

Abstract 4
Introduction: the joint JRC-EIT project 5
Summary of the workshop 7

1. Legal and Regulatory Implications of new and disruptive technologies: Autonomous Vehicles 11

1.1 Introduction 12
1.2 Licences for road testing 12
1.3 Product Safety and Standardisation 13
1.4 Data 14
1.5 Intellectual Property Rights 15
1.6 Liability, risk allocation and insurances 15

2. Assessment of Legal and Regulatory Implications of new and disruptive technologies: m-health 18

2.1 Scope 19
2.2 Data protection 20
2.3 Intellectual property (IP) 22
2.4 Cloud computing services 22
2.5 Medical devices 23
2.6 Liability and transformation of the medical profession 23
2.7 Other issues and challenges related to AI and m-health 24

3. Assessment of Legal and Regulatory Implications of new and disruptive technologies: text and data mining 26

3.1 Importance of TDM for AI 27
3.2 Legal framework of TDM 27
3.3 Intellectual property rules 28
3.4 Access to data and information 29
3.5 GDPR and data protection 32

Conclusions 33
Footnotes 34
References 38

ABSTRACT

AI will have numerous positive impacts on various aspects of our daily life, but it also presents several challenges. To fully benefit from AI potential, an appropriate regulatory and enabling framework needs to be put in place. This report presents the findings of a EIT/JRC joint project seeking to identify legal and regulatory challenges the usage of AI technology may bring for start-ups, in an attempt to raise awareness and knowledge about potential hurdles. The report contains the summary of the Workshop "Legal and regulatory implications of Artificial Intelligence (AI): the case" organised in this context, the three papers produced by the experts associated to the project and the project conclusions.

During the Workshop's plenary session, various speakers presented the EC policy landscape, gave concrete examples of EIT innovative projects, and examined the fundamental issue of liability for potential damages caused by AI systems. The experts' papers reviewed during the parallel session provide detailed insights on three specific sectors: notably autonomous vehicles, mobile-health and data mining. Thus the paper on autonomous vehicles tackles, among other issues, the implications of different licence's regimes for road testing, the lack of harmonised safety standards and the absence of a clear liability framework. From a more operational perspective, the expert's paper on m-health highlights concerns raised by the application of GDPR (General Data Protection Regulation) and provides further details on other aspects, such us the tension between portability rights and intellectual property, the application of the regulation on medical devices to m-apps, and the disparities in liability rules. Finally, the legal framework for the use and access to data for AI is explored in the paper on text and data mining. As a conclusion, a number of gaps have been identified across the sectors that may require adjustments in regulation, often on sectorial basis. Finally, it was noted that, when addressing them, policymakers should work closely with industry in order to produce relevant, useful, and balanced legislation.

INTRODUCTION: THE JOINT JRC-EIT PROJECT

The use of Artificial Intelligence (AI) to develop innovative solutions in business and for public good in society is becoming more common. New start-up companies that are focusing on this area are springing up all of the time and their use of AI suggests that the pace of change and the focus of such change is increasing dramatically. For example, the automotive sector has seen a huge surge in investment into connected autonomous vehicles (CAVs), with research into the potential uses of AI to help drivers in harsh weather conditions as well as developing driverless buses and trucks to transport people and goods alike. The Healthcare sector is looking at how AI can assist healthcare providers and individuals in everything from mobile app usage for self-diagnosis and health checking to the scanning of millions of patient records and x-rays to diagnose heart conditions and cancer.

These examples are an illustration of some of the start-up companies that have been supported by the EIT and who have also contributed to this project. The activities that these start-ups are involved in are representative of the types of activities where industry and academia are working together to harness the potential benefits of AI and other related technologies.

With such new technology comes a debate on how best to provide a framework within which developments can be harnessed for the public good and protect consumers. This was the case in previous technology revolutions and more often than not the pace of legislative change has not kept pace with that of technology change – and so in 2018 the European Commission published an AI strategy (EC 2018a), complemented by sectoral communications on mobility (EC 2018b) and ehealth (EC 2018c)[1] which looks to set out the future challenges to these sectors and the use of AI.

> *"The pace of change and the focus of such change is increasing dramatically"*

These challenges are being taken up by national legislatures as well and a number of countries around the world are looking to develop long term strategies to deal with digital transformations and the use of AI technology.

The aim of this joint EIC-JRC project is to take stock of existing initiatives and raise awareness of the regulatory and legislative challenges that faces society in general and new start-ups in particular when beginning to understand and put into production these new technologies.

The project focuses on three main areas where EIT supported start ups and projects have been particularly active: connected autonomous vehicles; m-health; and data mining. Within this context 10 EIT selected start ups were asked to fill-up questionnaires on legal and regulatory challenges they face when it comes to AI. On the basis of the responses to the questionnaire, desk research, and their own expertise, the three experts associated to the project - Chris Holder (Bristows LLP), Jean-Paul Triaille (EC DG JRC), and Jean-Marc Van Gyseghem (CRIDS) - produced a scoping paper in their respective field of expertise which outlined the existing and anticipated legal and regulatory challenges. These papers were validated at the workshop “Legal and regulatory implications of Artificial Intelligence (AI): the case of autonomous vehicles, e-health and data mining”, held at the EIT House in Brussels on November 23rd 2018. In addition, the workshop included a plenary session where EC policy initiatives, EIT innovation projects and liability issues were presented.

This report presents the final deliverable of the project. Section 3 contains a summary of the above mentioned workshop. Sections 4-6 follow with a series of experts’ papers that zoom into the specific sectors. At the end of the document, the overall conclusions of the project are presented.

SUMMARY OF THE WORKSHOP

On November 23rd, the Joint Research Centre and the European Institute of Technology co-organized a workshop in Brussels entitled "*Legal and Regulatory Implications of Artificial Intelligence*". Through presentations[2] and discussions among stakeholders, experts and policymakers, the content of the three scoping papers was thoroughly discussed as well as industry's concerns. Overall, it has been made clear that the challenge for legislators is to ensure that existing rules encourage and foster innovation rather than impede it. New laws and standards need to be developed to deal with any ambiguity or gaps in the existing legislative framework.

The first part of the Workshop was chaired by **Giancarlo Caratti**, Head of Intellectual Property and Technology Transfer Unit at the Directorate-General Joint Research Centre (European Commission) and **Michal Gorzynski**, Head of Section Impact at the European Institute of Innovation and Technology. It consisted in a plenary session where multiple speakers addressed the state of play of AI regulation, the legal challenges, and their respective actions in this field.

Cecile Huet, (European Commission, DG CNECT, Deputy Head of Unit, Robotics and Artificial Intelligence), took the workshop through the European Commission's outline for **AI Strategy for Europe** (EC 2018d) and also the funding profile for this area under Horizon 2020.

> *"The challenge for legislators is to ensure that existing rules encourage and foster innovation rather than impede it"*

Mrs Huet began by highlighting the potential positive impact that AI could have on the European economy and also the positive contribution that AI technologies could have on current societal challenges, including health, transportation, energy efficiency and cybersecurity.

Europe's leading position and its strength in the AI technology sector was discussed and the three main pillars for European AI strategy explained. They are:

- the boosting of technological and industrial capacity and take up of AI;
- the preparation for socio-economic change that will occur as a result of the wider use of AI;
- the necessity for an appropriate ethical legal framework to sit around AI.

For boosting capacity, investment in AI has to increase in order to fund the development of certain areas, including more R&D excellent centres, an AI-on-Demand Platform, digital innovation hubs and industrial data platforms.

Investment in this area is to rise from the current €4-5bn per year to a target of €20bn per year after 2020.

Following some detailed discussions surrounding the new **AI-on-Demand Platform**[3] and the development of the **Digital Innovation Hubs**[4] as well as additional funding opportunities[5], the workshop was presented with a general discussion on the ethical and legal framework that is to be required in order to support the rise of the European AI industry.
The **High Level Expert Group on Artificial Intelligence**[6] has been mandated to draft AI Ethical Guidelines for the development and use of AI as well as

a list of Policy and Investment Recommendations. Interaction with the group is facilitated through the creation of the **AI Alliance**, a European forum to engage in an open discussion on AI impacts and developments[7].

The interpretation of current regulations, for example the Product Liability Directive[8], were discussed in the light of a changing technology background. Further, the suitability of **safety and liability frameworks** were highlighted, with the future ability of machines to make decisions themselves being the subject of an **Algorithm Awareness Building** pilot[9] run by the European Commission.

The interrelationship between machines and intellectual property rights was discussed, with the question being asked as to whether AI could create and own intellectual property itself rather than as part of an existing corporation or licensor arrangement.

Alessandro Annoni, (European Commission, DG JRC, Head of the Digital Economy Unit) then introduced the role of the JRC and its views on the importance of AI as part of the JRC's *Flagship Report on Artificial intelligence from a European Perspective* (Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H, López Cobo M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L, 2018)[10].

Mr Annoni highlighted the growth in AI and its movement to the top of the technology innovation agenda across the world, its reliance on data to function, the future impact that it would have on society as whole, from jobs to power consumption and the potential dangers inherent in the use of data and its susceptibility to hacking and bias.
Mr Annoni concluded by recording how the challenges ahead were bigger than any single country could master on its own and the set out the importance of using Europe's values to develop the technology as an extremely important consideration to be taken into account. The launch of **AI Watch** to monitor the development, uptake and impact of Artificial Intelligence for Europe[11] was announced.

Michal Gorzynski then introduced the activities of the EIT and its vision to be the leading European initiative empowering innovators and entrepreneurs to develop world class solutions to societal challenges and to create economic growth and skilled jobs.

Through its Knowledge Triangle Integration approach EIT's links academic institutions, industry and research organisations in order to foster and develop innovations.

Michal presented the EIT's activities focusing on presentation of start-ups, innovation and education activities supported by the EIT in the AI field[12].

Maria Iglesias, (European Commission, Joint Research Centre, Legal Officer), focused on the objectives of this JRC/EIT project – to identify and discuss the legal issues raised by the use of innovative technologies in the three areas of study, namely CAVs, e-health and data mining.

The project was to use a combination of desk based research via the use of a question and answer document which was sent to ten identified start-ups in order to canvass their views on legal and regulatory awareness, needs and identified obstacles.

This information formed the basis of the scoping papers that, in turn, were used to focus the discussion on the parallel workshops held in Brussels.

Ceri Thompson, (European Commission, DG CNECT, Head of Policy Sector eHealth, Well-Being and Ageing), then provided a presentation on the **Communication on the Digital Transformation of Health and Care** (EC 2018b).
Mrs Thompson outlined the three major objectives of the European Commission in this area, being:

- the provision of better access to health data to European citizens;
- the use of digital services to enable more individual empowerment and person-centred care;
- the better connection between health providers and the better sharing of data to enable research, better diagnosis and better health care outcomes.

In order for this to happen, it was recognised that there should be better assistance made available to health authorities to enable them to scale up ‘best practises’, better support to start-ups and SMEs and more investment opportunities.

The role of data in such developments was outlined and the tension between **access to data and individual privacy** was seen as a challenge that required addressing. Cross border sharing of data – and specifically genomic data[13] – was discussed and recommendations highlighted around the creation of a European Exchange format for Electronic Health Records. In the striving for enabling citizens to access health records across the EU, the Commission will adopt a recommendation for Member States to align procurement plans in order to allow healthcare systems to ‘talk to each other and ensure interoperability.

In the field of mHealth, the Commission reported on a series of actions, notably the support provided to the **Code of conduct on privacy in mHealth**[14], the EU **mHealth Hub project** and the ongoing **study on the safety of non-embedded software**.

Daniele Rizzi, (European Commission, DG CNECT, Policy Officer, Data Policy and Innovation Unit), presented the 2018 Data Package and the Common European Data Space (EC 2018e)[15].

The size of the European data economy was set out, being in the order of €300bn in 2016 with a project to reach €1000bn by 2025 and the benefits of an open data economy highlighted – with the role of data within AI emphasized as key for the development of the AI industry and thus the creation of a ‘data space’ where all data could reside, be checked and be reused highlighted as a challenge for the future.

The better integration of government data, business data and scientific data, with no borders as potential boundaries, will be integral to the creation of a seamless data digital area with the scale to enable the development of new products and services based upon such data.

Antony Lagrange, (European Commission, DG GROW, Team Leader, Automotive and Mobility Industries Unit), discussed the 3rd EU mobility package with an emphasis on CAVs.

He set out the three main pillars of the EU’s vision, namely:

- the development of key technologies and infrastructure;
- ensuring that connected and automated mobility is safe;
- addressing societal concerns around jobs, skills and ethics.

The requirements for a safety framework were discussed, linked to the level of autonomy that any vehicle would have – the higher the level of autonomy, the more the requirement there could be for safety standards to deal with the ever decreasing role of the human driver[16]. The Commission has proposed a new **Vehicle General Safety Regulation** (EC 2018k), which addresses automated and connected vehicles in terms of perception, longitudinal and lateral control, driver monitoring, black box, platooning, and cybersecurity. The text is currently being discussed by the EU co-legislator. In addition, guidelines were put forward to facilitate the placing on the market of automated vehicles pending the adoption of fully harmonized requirements (EC 2018l).

The state of play of the ongoing discussions on legal issues around CAVs was introduced, in particular on **liability and insurance**[17].

Jean-Francois Aguinaga, (European Commission, DG RTD, Head of Surface Transport Unit) then introduced the research and innovation strategy for automated mobility in Europe.

This focused upon the strategy for development and deployment of connectivity and automation technologies for transport in Europe, the creation of short, medium and long term plans and also the eight thematic areas where initiatives were being focused. These included vehicle validation, large scale demonstrations of mobility solutions, physical and digital infrastructure and big data and AI[18].

In its proposal for Horizon Europe (EC 2018f)[19] EC has proposed a €100bn fund to invest in this area over the period 2021-2027 in order to boost Europe's scientific and technological bases and its innovations capacity, competitiveness and job creation.

Federico Menna, (Head of Innovation and Education Operations) and **Marina Samoylova**, (Innovation Analyst, EIT Digital, European Institute of Innovation & Technology) followed this by introducing the workshop to the EIT's digital activities on AI.

The definition of 'AI' was discussed and the fact that it is a rapidly developing and maturing market place.

Examples were given of start-ups that were working in such diverse sectors as warehousing (Autonomous warehouse and last mile delivery), cybersecurity (Security Operations Center for Critical Infrastructures), CAVs (Navya) and healthcare (KI ELEMENT, CheckPoint) but which were all utilising AI as a new technology to change the way that goods and services were being delivered and the implications for current rules and regulations was highlighted.

Gerald Spindler (Department of Corporate Law, Civil Law - Internet Law, Copyright and Telecommunication Law, Faculty of Law, University of Goettingen) then introduced his session relating to the **liability framework for dealing with 'smart' products**.

He started by highlighting the basic issue of 'foreseeability' and the problems associated with this legal concept when machines began doing things that they were not necessarily programmed to do. This, added to the complex digital environment where machines interact across networks and using software and data that may change during the course of a machine's activities or lifetime, exacerbate the technical legal issues of looking at 'who is liable'.

The suitability of the Product Liability Directive in this area was discussed. Does it deal satisfactorily with issues created by the use of new AI technologies?

Similarly, the concept of 'negligence' was examined and the inherent problems with looking at this as a legal concept when there are few, if any, societal norms and standards around the use of AI machines that can be applied at present.

The legal implications for tort law and contract law when dealing with these new technologies requires a great deal of thought across all jurisdictions.

The second part of the workshop was organized around three parallel sessions, each addressing one of the specific areas of the project - connected autonomous vehicles; e-health; and data mining. The three experts - Chris Holder, Jean-Paul Triaille, and Jean-Marc Van Gyseghem – kicked off their respective session by presenting the content of the scoping paper and then engaged in discussions with participants.

Thanks to the active participation of all participants to the workshop, the project team was able to receive significant feedback from stakeholders, and to take them into account during the redaction of the present report and in particular for the update of the three expert papers presented in the following sections.

LEGAL AND REGULATORY IMPLICATIONS OF NEW AND DISRUPTIVE TECHNOLOGIES: THE CASE OF AUTONOMOUS VEHICLES

Chris Holder, Partner for Bristows LLPs

1.1 Introduction

This scoping paper provides an outline of the most important challenges that the nascent autonomous vehicle industry face. These challenges are grouped together in five main headings, with various sub-categories and references to existing legislation and thinking.

This document has been prepared on the basis of desk research carried out by the author, complemented by his own knowledge, since the available information concluded from the questionnaire phase was scarce.

This scoping paper formed the basis of a workshop discussion held in Brussels on 23rd November 2018.

1.2 Licences for road testing

In order for autonomous vehicles to be viable commercial products, they must be tested on road networks as this is the only way for the technology to 'learn' about real world driving conditions. Clearly, testing can be done within labs and closed road circuits, but the training algorithms also need to have large amounts of 'real' data in order for them to work in 'real' situations.

There are a number of new developments as a result of the Horizon 2020 'Calls on Automated Transport' initiative and these include calls relating to human centred design for the role of drivers in highly automated vehicles and the efficient and safe use heavy commercial vehicles due in 2019 and 2020[20].

This requirement to test on the public road network must, therefore, take into account the fundamental requirement to keep the public safe when allowing autonomous vehicles to be tested on public highways.

As a starting point, one of the first areas to discuss is the licensing conditions that various governments around the world impose on the industry in order to balance out the need for testing against the need for public safety.
We will be first looking at what regulations exist, in

> *"How will it be ensured that the products that they are putting people in, and which are driving on public roads, will be safe for all to use and be around?"*

BOX 1. Key Figures

- "According to KMPG report "Autonomous Vehicles Readiness Index ranking countries' preparedness for AV adoption", the top five countries are: the Netherlands, Singapore, the USA, Sweden and the UK" (Peng T., 2018).
- "At least 33 US states have passed legislation, issued executive orders, or announced initiatives for the introduction of AVs on roads" (Peng T., 2018).
- "16 out of 33 jurisdictions have existing or proposed legislation, regulations or rules that address or apply specifically to driverless vehicles. 11 out of 33 jurisdictions have begun testing AVs in public, in private or both" (Baker McKenzie, 2018).
- Large scale testing is underway in Germany, France, UK, Sweden, Finland and Netherlands (EC 2018c).

Europe and elsewhere, which allow public road testing of autonomous vehicles, and second, we will try to understand whether more restrictive licences are a benefit or a burden to this new industry. Finally, we need to understand whether different regulations may create a situation whereby autonomous vehicle manufacturers would prefer to set up in one particular jurisdiction rather than another because of a lack of regulation – or whether this type of 'forum shopping' is, in fact, non-existent.

1.3 Product Safety and Standardisation

The safety of autonomous vehicles when they are driving on public roads is one of the most important issues to be discussed. How will it be ensured that the products that they are putting people in, and which are driving on public roads, will be safe for all to use and be around?

There is a pressing issue on what constitutes a safe autonomous vehicle because some of the technology being used has never been used before in such environments. Is there a recognised national or international standard that can be identified as being 'safe' when it comes to looking at the AI 'engine' that controls an autonomous vehicle and makes the on board driving decisions? The setting of minimum safety standards will be required which will then be used to set statutory safety laws and affect the way in which common law jurisdictions deal with concepts like negligence. It was recognised in the workshop, however, that not all situations can be tested

BOX 2. Product safety reference materials

European Union

The EU has the exclusive authority to set minimum safety standards for all new vehicles sold on the EU market. Safety features for automated vehicles in the EU are currently regulated by the General Safety Regulation (Regulation (EC) N° 661/2009).

Following a consultation process, the EU Commission on 17 May 2018 adopted a proposal for a revision of the General Safety Regulation – Regulation of the European Parliament and of the Council – safety requirements for cars (EC 2018k).

United States of America

US National Highway Transportation Safety Administration (NHTSA) guidelines: Automated Driving Systems 2.0: Vision for Safety (US Department of Transportation, 2017) – voluntary non-regulatory guidelines setting out a list of 12 essential safety elements, including vehicle cybersecurity, human machine interface and crashworthiness which manufacturers are encouraged to consider for system assessment, testing and validation.

a) Calls for each manufacturer and other entities engaged in testing or deploying AV technology to prepare a Voluntary Safety Self-Assessment (VSSA) and submit it to NHTSA for posting on the NHTSA website.

The workshop participants were very keen to point out the inherent dangers of not having a set of harmonised, international standards, especially for a multi-jurisdictional continent like Europe.

BOX 3. British Standards Institution's report: Connected and Autonomous Vehicles: A UK Standards Strategy (BSI and the Transport Systems Catapult, 2017)

Although there are very few existing standards specifically related to Automated Vehicles, there are specialised committees within standard developing organisations such as ISO with a large number of standards currently in development:

- ISO Technical Committee 204 - Intelligent transport systems
- CEN Technical Committee 278

BOX 4. Data reference materials

The GDPR: Regulation (Eu) 2016/679 Of The European Parliament And Of The Council Of 27 April 2016 On The Protection Of Natural Persons With Regard To The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive 95/46/Ec (General Data Protection Regulation)

United Kingdom law: Privacy and Electronic Communication (EC Directive) Regulations 2003 . PECR covers the processing of certain traffic data, amongst other things (Sec 7)

The German Automated Vehicles legal framework specifies that recorded data must be kept for 6 months, and in case of an accident for 3 years. However, the legislation has been criticised for not addressing data protection issues, including who is responsible for recording and deleting the data, and what measures are required to protect the recorded data against unauthorised access in the event the vehicle is sold (Freshfields Bruckhaus Deringer, 2017).

Norton Rose Fulbright raises interesting points regarding the apportionment of liability, and the export of personal data in their review of the UK legal landscape (Norton Rose Fulbright, 2017).

for before vehicles are put onto the market and so these might be a requirement for the adoption of a critical scenarios/ fail system approach.

3.4 Data

Given the amount of data that will be collected, analysed and transmitted by autonomous and connected vehicles, the industry will need to be prepared for dealing with an area which is not typically part of its remit – that of data protection and cyber security.

The data that will be collected will not just be used by the drivers of that vehicle. In order to provide additional services, and influence other areas such as road building and city development, data will also be used by other drivers, third party service providers, and governments. How will the industry deal with this transfer of data between individuals and other bodies, especially when autonomous and connected vehicles begin to cross international borders?

Cybersecurity

Cybersecurity issues will be a factor in both design and on-going deployment of autonomous vehicles. Given the obvious public safety concerns, governments, drivers, and manufacturers will want to be assured that the likelihood of computer hacking of

BOX 5.

US NHTSA's non-binding guidance: Cyber Security Best Practice for Modern Vehicles (Hatipoglu C., 2016) which includes a list of "fundamental vehicle cybersecurity protections," such as the control of keys and passwords, and control of access for vehicle maintenance diagnostics. The UK Government has also published its 8 "Principles of cyber security for connected and automated vehicles" (United Kingdom, Department of Transport, 2017).

How much responsibility makers will have to patch software vulnerabilities through software updates after the car has been sold?

In the Netherlands, the Dutch Consumer's Association has filed a lawsuit against Samsung for failing properly to release updates to its smart phones running on the Android OS. If this lawsuit prevails, it is difficult to see how the same principle would not be applicable to connected cars.

Cyber-attacks still do not represent the main threat to data security. Employees and contractors have long been, and will likely continue to be, the cause of most data security breaches, with 60% of attacks in 2015 being found to be an 'inside job'.

vehicles is negligible.

The workshop participants identified the relationship between the need for data privacy and security on the one hand and the socio-economic benefits of automated vehicles on the other as being an issue. As automated vehicles become more widely used by the public and 'connected' to other vehicles and/or non-vehicular networks, the need for free access and sharing of information between vehicles increases but, of course, data privacy and security issues increase.

The vast amounts of data generated by automated vehicles create a new enticing target for hackers and other cybercriminals such as criminals seeking information about the automated vehicle itself to sell to competitors, or wishing to infect the automated vehicle with a virus or malware in order to extract ransom money.

1.5 Intellectual Property Rights

The protection and exploitation of intellectual property rights is of key concern to new companies operating in a new area. For start-ups in the autonomous vehicle industry, there is a general concern on how to protect their ideas and inventions, especially when dealing with companies from foreign jurisdictions. This issue is one of many that will be decisive to the future growth and economic viability of a start-up in this industry.

> *"The use of technology that is the subject of existing patents, particularly in the field of mobile communications, will open the door to potential litigation between AV manufacturers and operators and those companies that hold those patents."* Bristows LLP

Not only will intellectual property issues associated with patents, copyrights and trademarks be worth discussing, the ownership of data and databases which will be developed and used by autonomous vehicle companies also needs to be addressed (Pinsent Masons, 2016).

The ownership of Intellectual Property can be transferred between the creator and the purchaser, or it can be licenced. These are two different and separate means to trade intellectual property rights and the way that technology for CAVs will evolve will rely on them both.

When licensing an algorithm or data, the licensor may impose a number of restrictions that may have serious commercial ramifications if a company is not aware of the terms of the licence. There may be other legal considerations, for example in competition law.

Furthermore, there are different types of IP rights in the field of new technology which will have to be taken into account such as patents, copyrights, design rights, trade marks, database rights, etc. Each of them can be examined independently of the others and is regulated by specific regulations and laws, all of which will be relevant to businesses operating in the CAV industry sector.

The workshop participants were also keen to emphasise the issues that arose when discussing the creation of IP by machines themselves. Who would own such IP in these circumstances? The machine? Or the car manufacturer?

1.6 Liability, risk allocation and insurances

New technologies at the heart of the autonomous vehicle industry change the way machines operate in the real world, and raise the real prospect of machines making decisions without a human being directly involved. How will the industry deal with the many issues surrounding fault, damage and liability?

Commercial contracting between suppliers should also be discussed given that manufacturers will be able to offset risk via commercial contracts with suppliers up and down the chain. An understanding of how to contract when dealing with complex computer systems, hardware and software, will be advantageous.

BOX 6. Data reference materials

What is the existing legislation regarding liability for product safety issues?
The basis for most regulations related to self-driving cars is the 1968 Vienna Convention on Road Traffic. One of its fundamental principles is that a driver must be fully in control of and responsible for the behaviour of a car in traffic. In March 2016, the convention was amended to include autonomous vehicles, but only if the automation technology is conformed to the UN vehicle regulations, and that the driver can override or switch off the technology. While sharing the same fundamental basis, regulations across Europe remain fragmented.

United Kingdom:

The UK Consumer Protection Act , (based on the Product Liability Directive , which is the basis of all product liability legislation in Member States) imposes strict liability on manufacturers for defective products. Under strict liability the injured party is not obliged to establish fault with a product, but must only show that a defective product caused the loss. A product is defective under the UK Consumer Protection Act if "the safety of the product is not such as persons generally are entitled to expect" taking into account the purpose for which the product has been marketed, any instructions for use or warnings, what might reasonably be expected to be done with the product at the time when the product was supplied – a product is not unsafe simply because a safer product was later developed or industry safety standards were raised after it was supplied.

In 2017, Taylor Wessing noted the following (Wessing T ., 2017):

"The test is, therefore, one of consumer expectation and this will be more complex in the context of autonomous vehicles where users are unlikely to have any significant understanding of the technology products used. As to their expectations on safety, these could be higher or unrealistic. Manufacturers will need to ensure that they inform consumers sufficiently as to how the automated features should be used safely and explain any potential risks. Manufacturers and software providers should consider taking advice on the formation of product instructions and warnings given to consumers with the automated vehicles (particularly in the user manuals) as such documents will become increasingly important in the context of product liability claims."

What is the existing legislation regarding driver negligence?
In the UK, there currently is no legislation taking into account automated vehicle technology in the allocation of criminal liability for road traffic accidents and offences. The Road Traffic Act 1998 refers to the "user" as being liable for the car's actions, but this will require review in light of the changing technology. The Law Commission is carrying out a three year project to review who should be blamed for road accidents caused by driverless cars and criminalising hackers who target autonomous vehicles.

The German automated vehicle legislation does not require drivers to remain focused on the road at all times, but they must be able to react "without undue delay" if the system prompts them to do so, or if they themselves realise that this is necessary. Both driver and owner remain liable even if the vehicle is in automated driving mode. However, drivers are able to avoid liability if they are found to have lawfully used the automated driving mode (automated vehicles must be equipped with a "black box" to identify whether it was the driver or the system which had control at the time of an accident) (KWM, 2017). Insurance has a part to play in this, and it will be therefore interesting to understand which insurance policies may be developed to cover future liability. Governments are looking to insurance companies to provide answers for the market and in some instances have produced legislation to cover these points.

Furthermore, it will be of interest to understand how insurers approach the pricing of risk in this regard, especially given the fact that this is an entirely new area for them.

Is there any specific law for insuring automated vehicles in the EU?
"The appropriation of risks in relation to the use of motor vehicles is currently regulated through two main EU legislative acts

governing liability: the Motor Insurance Directive (2009/103/EC) and the Product Liability Directive (85/374/EEC). This system is based on the highly harmonised EU framework for liability of a producer of a defective product and provides for a very limited EU framework (mainly establishing third-party liability insurance cover and procedure for claims resolution) on civil liability for victims of road traffic accidents. When it comes to the substantive rules relating to road traffic accidents, national rules on liability and the calculation of damages for victims apply." (Evas T., 2018)

UK's 'Automated and Electric Vehicles Act 2018':

- Extends compulsory motor vehicle insurance to cover the use of automated vehicles in automated mode.
- Refers only to roads or other public places, which means that the insurance position for accidents on private roads and estates is unclear.
- Adopts a single insurer approach by which the injured party would claim only against the insurer and not the vehicle manufacturer. The insurer can then itself recover the sums from the manufacturer.
- The insurer's liability is limited in cases of contributory negligence and there is no insurer liability for accidents caused by the owner's "negligence in allowing the vehicle to drive itself when it was not appropriate to do so".
- Insurers are permitted to exclude or limit their liability for damage suffered as a result of prohibited software alterations or failure to install safety-critical software updates.

Other Jurisdictions

There are a number of jurisdictions that have "no fault compensation schemes" and these may prove to be a more successful model than "fault based" regimes based on the tort system (Schellekens M., 2018).

ASSESSMENT OF LEGAL AND REGULATORY IMPLICATION OF NEW AND DISRUPTIVE TECHNOLOGIES: M-HEALTH

Jean-Marc Van Gyseghem, Research Director and scientific coordinator,
Research Centre Information, Law and Society (CRIDS) –
Member of the Bar of Brussels

2.1 Scope

This scoping paper aims to provide legal insights about e-health and, more specifically on mobile health applications (hereafter m-health). AI is more and more used in clinical trials to improve research which raises various issues.

The paper highlights the main legal issues raised when using m-health applications powered by Artificial Intelligence[21] (AI) in health care. The analysis is based on the legal state of the art regarding m-health and AI as well as the perceptions of companies active within the field.

2.2 Data protection

The switch from intra muros to extra muros healthcare involves multi-disciplinary interactions between physicians and non-physicians regarding their respective access to health data. It also involves new actors, such as *"app developers, operating system (OS) manufacturers and device manufacturers, app stores and third parties (e.g. advertisers)"*[22]. m-health apps must comply with the General Data Protection Regulation, (hereinafter GDPR)[23] and 'privacy streaming', both referring to the concept of necessity and proportionality (e.g. Article 8, European Convention on Human Rights). This means that the use of anonymised data should be favoured, or at least the use of pseudonymised data[24]. The use of non-pseudonomised data should be reduced as much as possible and data should be pseudonomised or anonymised as soon as possible. The principle of minimisation is highly connected to the concept of pseudonymisation as both pursue the same objective of minimizing interference in the right to privacy (Van Gyseghem J.-M., 2016). In other words, only necessary data is allowed to be processed.

"The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed"[25]. The GDPR is built inter alia, around this concept of necessity, also visible in many provisions such as Articles 4.1, littera C with the concept of 'adequate data', Article 6, Article 9, etc.

Besides this, there is a concept of empowerment that consists in giving more control on their data to the data subject/patient. This concept is highly connected to the rights given to the data subject as analysed below. But if the patient has more power, does it mean that she/he has more responsibility? Nothing could be less certain.

Consent in data protection

In many cases, the processing of users' health related data in a m-health framework is based on the explicit consent (see art. 7, GDPR) even if other legal basis for processing health related data are possible. As specified in Recital 32 regarding Article 7, *"consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement."* Article 7 should be read together with articles 12 to 14 dedicated to information[26].

In an AI environment[27], it seems that data subjects' information[28] might not be clear enough, as it does not touch upon the logic involved in the algorithms used to run AI. This might be a real issue in relation to IP concerns (see below), as the creator/designer/producer/developer may be reluctant to disclose information covered by IP rights.

BOX 7.

Consent can be a major issue, either regarding shared principles on health law within the European Union or with respect to the GDPR.

Even if the consent is not used to base the processing, adequate and complete information is still needed.

The concept of consent is important in healthcare beyond the data protection perspective, as an aspect of self-determination of the patient[29].

When analysing m-health applications, we found that patients will usually not get access to the application without having consented to the mobile health application's terms. It can also be observed that in many applications, the information provided to the patient is in English and appears to be the only source of information for the patient/data subject. Depending on circumstances, this might be an obstacle to achieving valid informed consent, as many patients have a limited understanding of English and therefore may not understand what the application requires. Thus, there is a risk that consent is not sufficiently informed in the sense of article 7, GDPR[30].

Other issues

The GDPR raises multiple other issues for companies active in the domain of m-health[31]:

- In terms of security, the GDPR requires the implementation of technical and organisational measures to ensure a high level of security. It provides that *"taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing".* (Dumortier F., 2018)

- Some companies find that security measures (such as multi-authentication[32]) constitute "a serious additional barrier", in particularly when dealing with big groups of users. Another issue linked to security measures concerns the length of the password, which have been a source of complaint from users due to the intrinsic complexity (IT provides technological solutions for handling multiple passwords).

- The use of emails has been an additional source of complaints: physicians using data collected from applications would like to receive them by email (which is inadequate in terms of confidentiality) rather than through a secured link protected by a password. Indeed, many emails containing sensitive data are not or not sufficiently protected (i.e. encrypted), which could constitute a major security breach. This issue concerning a major communication channel constitutes an additional barrier to the use and development of m-health.

- Some new rights formalised by the GDPR are difficult to implement, for example:

  The 'right to erasure' ('right to be forgotten'): companies have highlighted that they do not have enough information regarding the identity of the users to comply with such right, which may become an issue.

  The 'right to data portability': GDPR puts in place a right to data portability[33], which means that data subjects will have the right to receive the personal data concerning them, processed by automated means, that they have provided to a data controller. This new right gives more power to data subjects as it facilitates the possibility to move, copy and transmit their personal data from one IT environment to another[34]. Consequently, this right is applicable to data actively provided by the data subject and the ones resulting from the observation of an individual's behaviour. In contrast, personal data generated by analysing the behaviour of the data subject is not covered by the right to data portability[35] as it is for a credit score, or the outcome of an assessment regarding the health of a user[36]. This right could be an issue as it may prove difficult, in an AI environment, to separate data covered by the portability right and data that are not. Which data are genuinely generated by AI and which data has the data subject 'actively' provided? Portability is also related to interoperability. Indeed, Recital 68 of the GDPR points that "data controllers should be encouraged to develop interoperable formats that enable data portability".

- The cost (registers, analysis, lawyers, etc.) that the implementation of the GDPR implies, have been highlighted as an issue by some companies (mainly SMEs).

"In the context of m-health, data processing could involve various risks for the data subject's rights and freedoms, requiring companies to comply with the privacy by design obligation"

BOX 8.

Companies, in particular SMEs, find difficult to properly implement the GDPR in the field of m-health.

AI raises additional questions, such as the implementation of the right to portability, etc.

It also implies an issue at the cost level.

Privacy by design and by default is another important aspect in the creation of software processing personal data. This means that the data controller should *"implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data"*[37]. This should be done *"both at the time of the determination of the means for processing and at the time of the processing itself"*[38]. To comply with this obligation, the data controller should account for *"the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons [ed.: data subject) posed by the processing"*[39].

It is evident that in the context of m-health, data processing could involve various risks for the data subject's rights and freedoms, requiring companies to comply with the privacy by design obligation. This duty is put on the data controller (companies processing data for their own purposes), but also indirectly on the creator/producer who has to deliver a product that can be used confidently by the data controller[40].

The recent Declaration on ethics and data protection in artificial intelligence adopted by the International Conference of Data Protection and Privacy Commissioners (ICDPPC) on October 23rd 2018, also needs to be underlined here (International Conference of Data Protection & Privacy Commissioners, 2018a). This declaration promotes, among other things, the *"adoption of an international approach and standards, in order to ensure the promotion and protection of human rights in all digital developments at international level"*. The Declaration is now open to public consultation (International Conference of Data Protection & Privacy Commissioners, 2018b).

2.3 Intellectual property (IP)

M-health developers usually rely on intellectual property (IP) rights or other legal and technical protections for their licensing strategy. This may create tensions between the need to create new applications and the need to protect investments.

It can be observed that many companies are not in favour of licensing their product under an open scheme such as open source. This trend finds its justification in the fact that innovation needs IP protection to remunerate investments in creating the system/application. The reluctance seems even stronger when dealing with algorithms such as those used in the field of AI where competition is strong. Indeed, such creations are at the core of the business model of many companies.

This reluctance to licence under open schemes might affect the principle of portability that may request knowledge of each system, in order to allow people to change service provider without any barriers, thus potentially impacting the follow-up care of patients changing service provider. As highlighted by Graef, Husovec and Purtova (Graef I., Husovec M. & Purtova N., 2017), portability might come to clash with IP protection rules.

BOX 9.

IP might raise issues regarding:

- Interoperability between different systems used in e-health
- Locked/closed systems, which could be negative for the patient and the physicians
- Use of open data

Furthermore, this lack of openness may reduce the amount of data available to improve algorithms used in the AI systems. Indeed, such algorithms need to be fed in order to be improved and the only food is real data. If such data is reduced, the evolution of algorithms could be reduced and as a consequence, there could be a reduction in quality of the algorithms as well as in competition. This could mean that only big companies have the ability to improve algorithms - which would impact competition and may reduce the quality of services or generate increased costs.

Voices now clamour and plead for the use of open data in order to feed AI. Such a use will allow smaller entities to be able to develop systems with less constraints. For the record, Europe promotes open data as an instrument for research.

2.4 Cloud computing services

Cloud computing services are often used in m-health and the cloud computing services platform can be private, public or hybrid. The use of public clouds raises major issues regarding data protection, especially for sensitive data (e.g. health data). Most of the contracts with cloud service providers are pre-formulated, which gives no room for negotiations. Thus, this potential lack of control concerning the contractual clauses can be in conflict with the obligation for the data controller to have a data processor (e.g. the cloud services provider) that provides *"sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the require-*

ments of [the GDPR] and ensure the protection of the rights of the data subject"[41]. Indeed, the client has no capacity/power to adapt the contract to its own risks. To avoid any risk regarding data protection, some companies subscribe to contracts with cloud providers specialised in hosting healthcare data. However, companies, mainly SMEs, are asking for a model-contract to be used when subscribing to cloud services, which could provide benefits for SMEs using these services.

2.5 Medical devices

Regulation (EU) 2017/745 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC *"lays down rules concerning the placing on the market, making available on the market or putting into service of medical devices for human use and accessories for such devices in the Union. This Regulation also applies to clinical investigations concerning such medical devices and accessories conducted in the Union"*[42]. A medical device is for the purpose of this regulation defined as *"any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings"*[43] mainly for *"diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease"*[44]. The main objective of this piece of legislation is *"to ensure the smooth functioning of the internal market as regards medical devices, taking as a base a high level of protection of health for patients and users"*[45].

This definition might be applicable to most of the AI applications used in m-health, mainly when dealing with AI incorporated in software, which is often the case[46]. However, the producer may have difficulties in knowing if the application is a medical device or not (as opposed to an accessory to a medical device)[47]. If the AI application is included in the definition of medical devices in the 2017/745 Regulation, companies have to comply with CE marking, information duties, etc[48]. However, this seems to be largely unknown by producers. Besides this lack of knowledge, the cost for the administrative steps in obtaining the CE marking may in some instances be an issue.

Some actors on the field raise the issue related to the fact that Health related mobile apps are available on app stores without control on the quality. This might lead to insecurity (e.g. break of confidentiality, safety obligations, etc.) and lack of trust in product. To avoid this, an app store dedicated to health related apps might be accredited so to create a kind of label.

2.6 Liability and transformation of the medical profession

It is evident that the medical profession is changing and m-health is one of the elements of this transformation. Using mobile applications in the m-health and AI environments raises liability questions at several levels. However, this issue is usually dealt with at the national level and the answers can differ from one Member State to another (Ferrara S.D. & Baccino E., and alii, 2013)[49]. Allocation of responsibility is often tackled through contractual means that intend to protect actors towards their own liability.

Producer

The liability of the producer of the software/product is put at the level of the device/software that has to be compliant with the applicable legislation, such as:

- Regulation (EU) 2017/745 on medical devices (see above);
- GDPR with the concept of privacy by design (see above).

Regarding the first point and if the product falls under the medical device definition, the producer has to provide a safe product in the sense of Regulation 2017/745. *"Product safety and liability are complementary legal frameworks aiming* *to provide trust and safety to consumers."* (EC 2018g)

The second point concerning data protection might raise a different question: what kind of guarantees have to be given by the producer and what kind of liability does it imply? The following two hypotheses can be drawn from this:

- The producer is both the company operating the software and the algorithms: This situation should not raise any question, as the GDPR is quite clear in this case. The producer/owner is forced to adopt a privacy by design approach and would be responsible for any damage caused by its software in regards to the GDPR; or
- The producer and the operator are two different entities: In this case, the GDPR might not be sufficiently clear. Indeed, the GDPR deals with the data controller and the data processor but not with entities, which are none of them, but nonetheless produce the software processing personal data[50]. In this case, the existing contractual relationship between the producer and the operator should be analysed. This contract should fix the duties of the producer. Companies using software produced by a third party are often advised to highlight this point in their contract and, in case of procurement contracts, in their requirement specifications.

Physician

Physicians may have troubles in processing information received from various devices due to numerous and diverse messages. A major risk constitutes loosing crucial information hidden by less relevant information. Who would be responsible for any damage to the patient in such a situation?

Another situation concerns the physician taking a decision based on inaccurate information delivered by software (i.e. a faulty algorithm). Bearing in mind the below mentioned caveat, physicians will have to go after the producer/operator of the software.

BOX 10.

Liability rules are mainly at the level of the Member States, which creates inconsistency at the European level and therefore discomfort to the relevant actors.

Many applications contain specific contractual provisions on liability in the absence of any specific legislation dealing specifically with liability in m-health.

Patient

Patients might misuse the device, which could send inaccurate information and induce wrong medical intervention (and damages to the patient's health). What kind of liability would this entail? Would liability be allocated to the patient or would it be shared between several actors (e.g. based on a lack of information)?

2.7 Other issues and challenges related to AI and m-health

During the workshop held in November 23th, participants proposed European initiatives such as EU regulation on standards that could be under the form of a framework regulation reinforced with soft law. Participants also evoked the idea of having specific bodies such as an European AI Agency/Ombudsman addressing new technologies and legal issues or an European Ethical Approval Committee dealing with e-health and m-health app.

AI is also significant in scientific research as showed by several projects launched in Europe. GDPR provides for specific rules in matter of research in order to facilitate it and avoid additional barriers. However, GDPR still requires balance between using personal data and promoting research[51].

Due to the limited scope of this project, this paper does not focus on the following areas although they can be of relevance in this context:

- Consumer rights – relevant questions concern the qualification of people using m-health services: are they consumers, patients or both? Answering these questions is fundamental as it will affect applicable legislation. The Directive 2011/83/EU of 25 October 2011 on consumer rights will not be applicable in matter of contracts in healthcare[52].
- Social health insurance – Member States might consider the reimbursement of health services provided through m-health by social security. This question is, for example, analysed by the Belgian government in the "The Belgian Digital Health Valley" framework.

ASSESSMENT OF LEGAL AND REGULATORY IMPLICATION OF NEW AND DISRUPTIVE TECHNOLOGIES: TEXT AND DATA MINING

Jean-Paul Triaille, Directorate-General Joint Research Center (JRC),
European Commission,
Brussels, Belgium

3.1 Importance of TDM for AI

This scoping paper draws on the responses given to the questionnaire and further relies on desktop research and in-house experience on TDM, as well as on the workshop which took place on November 23, 2018.

Many definitions have been proposed of TDM (Triaille J.P., de Meeus J., de Francquen A., 2014).

In a report for the European Commission, the following definition had been proposed:

"the automated processing of digital materials, which may include texts, data, sounds, images or other elements, or a combination of these, in order to uncover new knowledge or insights" (Triaille J.P., de Meeus J., de Francquen A., 2014).

TDM (or data analysis) is done by applying automated techniques to a set of selected digital materials; "automated" is opposed to "made by humans" and it is indeed this characteristic which makes TDM so powerful and which raises new IP (intellectual property) issues; TDM involves the processing of data, which may (but this will not always in every case) include the extraction, copy, comparison, classification or other statistical analysis, etc. of data, or a mix of them; it can be applied to all types of contents and in most cases, the interest of the process is to include a large number of materials. The technique may be applied in very different for-profit and non-for-profit contexts, across sectors, and by different actors, from research organisations to start-ups, big companies, journalists or citizens.

"The development of AI leads to a growing relevance of TDM regime and of its possible weaknesses"

"The legal framework of TDM is mainly impacted by intellectual property rules and, in certain areas ... by privacy rules"

In the recent JURI Report adopted by the European Parliament on the draft copyright directive, the definition which is proposed reads as follows:

> *"text and data mining' means any automated analytical technique which analyses works and other subject matter in digital form in order to generate information, including, but not limited to, patterns, trends and correlations"* (EC 2016).

It is easy to understand that TDM is an essential component of many AI projects and that, because AI and machine-learning do require to process large amounts of data, the legal regime applying to TDM can have an impact on the future development of AI and on the possibilities by start-ups to engage in AI projects. The development of AI leads to a growing relevance of TDM regime and of its possible weaknesses[53].

3.2 Legal framework of TDM

The legal framework of TDM is mainly impacted by intellectual property rules and, in certain areas (i.e. where "personal data" are being processed), by privacy rules (which we will however not address here in any significant depth). In addition, the question of access to data is also more and more important, both from the private sector and from the public sector. We will address hereafter both intellectual property (IP) rules and issues related to access to data.

3.3 Intellectual property rules

TDM unavoidably implies some copying of the materials. Often, TDM will require accessing and processing materials that are protected by copyright (e.g. when TDM is being made in relation to written publications or original images) or by the database maker *sui generis* right. In many cases, TDM will target publishers or data providers' databases, but, in many other cases, it may also concern scraping of publicly available websites that, in spite of being freely accessible, may also be protected by copyright or the *sui generis* right.

In order to avoid that copyright becomes a hindering factor to the development of TDM, several legislators have proposed to introduce a TDM exception in copyright legislation. In the EU, this has been the case in the UK, in France, in Estonia and in Germany (Geiger C., Frosio G. & Bulayenko O., 2018). The European Commission has also decided to propose an exception for TDM (EC 2016).

The text of the draft directive as adopted by the EC was proposing to have a binding exception (not waivable by contract), applying in all MS and benefitting research organisations. Research organisation is defined as:

> *"a university, a research institute or any other organisation the primary goal of which is to conduct scientific research or to conduct scientific research and provide educational services:*
> *(a) on a non-for-profit basis or by reinvesting all the profits in its scientific research; or*
> *(b) pursuant to a public interest mission recognised by a Member State;*
> *in such a way that the access to the results generated by the scientific research cannot be enjoyed on a preferential basis by an undertaking exercising a decisive influence upon such organisation".*

The exception makes no distinction between commercial research and non-commercial research, and research organisations would also benefit from the exception when they engage into public-private partnerships. Because TDM also involves extraction of data and thus possible infringements to the *sui generis* right of database producers, the exception would also cover this *sui generis* right.

The text has evolved during the discussions in the European Parliament and in the Council, and amongst several other options, it is now envisaged to extend the benefit of the exception to educational establishments and cultural heritage institutions conducting scientific research.

A critic expressed to the text is that it benefits only research organisations and not commercial companies. However, one of the versions being discussed in the trilogue discussions would allow Member States to go further. A new proposed recital states that *"To encourage innovation also in the private sector, Member States should be able to provide for an exception going further than the mandatory exception…"* (new recital 13a), and Member States would have the possibility to allow TDM also by the private sector and for commercial purposes, via the "optional exception or limitation for text and data mining" of the proposed new article 3a.

This additional exception would be optional, each Member State being free to adopt it or not.

The exception would however not apply when the use of the materials has been *"expressly reserved by their rightholders, including by machine readable means"*[54]. It means that for instance, on a website, the terms and conditions could still validly prohibit TDM being made of the contents of the website.

Another critic was that the text does not benefit individual researchers; the text amended in the European Parliament would however allow Member States to continue applying the existing possible exception for non-commercial scientific research to individual researchers.

The issue will continue being discussed in the context of the trilogue between the EC, the European Parliament and the Council.

Some concerns have also been expressed about the consequences of Brexit and the possibility that the UK might decide to adopt a more flexible exception, more along the lines of the US "fair use" (Jondet N., 2018).

It is worth noting that when a possible TDM exception at EU level was first discussed, in 2014, it was not in the broader context of artificial intelligence and machine-learning, and those words do not appear for instance in the two reports which were commissioned by the European Commission (Hargreaves i. et al., 2014), even if TDM was then already seen as a promising field which had to be nurtured and if the growing importance of data to the economy was obviously the background of these studies. In addition, many discussions around TDM focused initially on the mining of scientific literature, with less emphasis on the importance of the information generally available on the Web: with the increasing diversity of AI applications, it is the Web itself which becomes the main source of data, and less so the journals published by scientific publishers.

What comes out of the questionnaire by EIT and JRC?

Both start-ups mentioned IP as an area of major concern to their activities, and as an area in which they will seek further legal advice in the near future.

Both also mention that they refrain from using the contents of websites where the terms and conditions prohibit TDM or webcrawling.

As it stands, they would not benefit from the TDM exception as proposed in the initial text of the draft directive, except where the activity would take place in the context of a joint project (PPP) with a university or research organisation (in which case, the beneficiary of the exception would still have to be the university or research organisation).

They would benefit from the optional exception proposed in the trilogue discussions but only in the countries where the exception would have been introduced. When a website would prohibit TDM or webcrawling of its contents, this would still have to be taken into account, and the exception would not apply.

If in the end an exception was introduced for the benefit of start-ups, the question would then be how the concept is defined (turnover, number of years of existence, number of employees etc.).

It appears that the start-ups are not very well informed about the debates on the TDM exception, while recognizing their importance for their business, the TDM exception being "useful in order to avoid imposing unreasonable burdens to data-related research".

One of the main challenges mentioned consists of "the web crawling and scraping restrictions led by the GDPR and intellectual property rights", which they would like to see applied in a reasonable manner "so as not to block data-driven innovation". In its response, one of the start-ups insists that "new regulations, if necessary, should take into consideration the asymmetry of power between big and small platforms and protect incomers".

3.4 Access to data and information

The TDM exception, in whichever manner it ends up being adopted, is still just an exception and does not create a right to access the information. On the contrary, it has always been drafted in such a manner that it was limited to contents to which the user had first obtained lawful access.

Even in its most liberal interpretation by the proponents of the idea that "the right to read is the right to mine", the right to read would not in itself create a right to require access to data that is not made freely available.

Also, under the "optional exception" solution proposed by the JURI Committee in the European Parliament, the contents would also have to be first lawfully accessed, and rightholders (including website owners) could still decide to "reserve" the use, including by machine-readable means.

With the advent of AI, the issue of access to data and information has grown in importance. The issue covers two sets of questions, first vis-à-vis public sector information and secondly vis-à-vis privately-held data (Osborne C., 2016)[55].

While discussions on ownership are still very much undecided, the issue of access to data has indeed gained prominence in the debate and many commentators consider that some rules on access to data should be introduced. And indeed, *"the problem of rights of access to data might be a much more important future research topic than the question of exclusive ownership"* (Kerber W., 2016). With an increasing share of data in the digital economy being held privately, *"the problem of access to data will be one of the pivotal future policy questions for the governance of the digital economy"* (Kerber W., 2016).

Discussions in the EU first started about the ownership of machine generated data (see the *Communication on Building a European Data Economy* (EC 2017a), where the EC put forward a series of legislative and non-legislative options for discussion, among them the possible creation of a new data producer's right. In the later *Communication, Towards a common European data space* (EC 2018e), the EC focuses no longer on ownership of data but on access to data. A series of measures have been adopted (the "data package"), including:

- for *public sector data*: a proposal to review the PSI Directive (EC 2018j);
- for *research data*: a recommendation on access to and preservation of scientific information (EC 2018h), and
- regarding *access to data by the private sector*: a guidance document on the business-to-business and business-to-government exchange EC 2018i).

Discussions on a possible right of property on data are somewhat speculative or theoretical, but issues of access to (or refusals of access to) data are more concrete and can be the object of more empirical analysis (as they can be observed in practice or by economic studies). Even in the absence of a new ownership right indeed, questions of access to data may arise: requests to access can face *de facto* monopolies on data (combined sometimes with technical protection measures and confidentiality precautions).

The other side of the coin, if discussing access to data, is "data sharing".

The question arises then as to whether any legislative intervention in this field should be sectorial or rather horizontal. Commentators generally agree that "data markets" each present very different and specify characteristics, in terms of business models, actors, strategic importance of the data, etc. This leads to the rather widely shared recommendation that sector-specific regulations should be preferred to a general "one sits fits all" regime of access to data, at least as a first step (Kerber W., 2016 ; Kerber W., 2017[56]; Mezzanotte F., 2018[57])

A combination of one general access regime (mainly defined in function of objectives) with some sectorial regulations (rather defined in terms of beneficiaries) has also been advocated (Mezzanotte F., 2018). While the possible introduction of new mandatory rights to access privately-held data is considered as a delicate issue, a number of sectorial regulations already foresee some sorts of rights to require access, for specific purposes (Osborne C., 2016)[58].

Commentators generally favour a *"minimal regulatory approach to foster B2B data sharing"* (Benelux E., 2018 & Osborne C., 2016); the JRC has recently indicated in a recent report that it considered a possible regulation as premature and that it therefore *"offered no policy conclusions"* and stated that *"more research is required to bring economics up to speed with these questions"* (Duch-Brown N., MartenB. & Mueller-Langer F., 2017).

For public sector information

Following an impact assessment and various public consultations, the European Commission has published a draft directive reviewing the existing PSI Directive (EC 2018j). The main changes to the existing framework have been presented as follows in the explanatory memorandum to the text:

> *Dynamic data/APIs*: a 'soft' obligation for Member States to make dynamic data available in a timely manner and to introduce APIs. For a limited number of fundamental high-value datasets (to be adopted through a Delegated Act) there will be a hard obligation to do so.
>
> *Charging*: tighten the rules for Member States for invoking the exceptions to the general rule that public sector bodies cannot charge more than marginal costs for dissemination. Create a list of fundamental high-value datasets that should be freely available in all Member States (same datasets as above, to be adopted through a Delegated Act).
>
> *Data in the transport and utilities sector*: only public undertakings will be covered, not private companies. A limited set of obligations will apply: public undertakings can charge above marginal costs for dissemination and are under no obligation to release the data they do not want to release.
>
> *Research data*: Member States will be obliged to develop policies for open access to research data resulting from publicly funded research while keeping flexibility in implementation. The PSI Directive will also cover research data that have already been made accessible as a result of open access mandates, focusing on re-usability aspects.
>
> *Non-exclusivity*: transparency requirements for public-private agreements involving public sector information (ex-ante check, possibly by national competition authorities, and openness of the actual agreement).

This would, if adopted, bring about a number of improvements to the TDM sector, notably the increased use of APIs by Member States, which will facilitate identification and processing of datasets, and the future availability of much more research data.

For access to privately-held data

The Commission hopes that the principles of the guidance document mentioned earlier (EC 2018i) will be respected in contractual agreements, to ensure fair and competitive markets for the IoT objects and for products and services that rely on non-personal machine-generated data created by such objects, but will continue to assess whether amended principles and possible codes of conduct are sufficient to maintain fair and open markets. If necessary, the Commission indicated that it would take appropriate actions but it is considered that at this early stage of development, it is not yet possible to decide what the standard and/or fair practices in the field are (Graf von Westphalen F., 2017).

What comes out of the questionnaire by EIT and JRC?

In the responses to the questionnaire, data access is mentioned as a legal area of major concern today and as an area in which the start-up will look for legal advice in the near future.

This partial feedback by the start-ups is comforted by other consultations. It seems that market operators view issues of access to (and re-use of) data as more important and more impacting for them than (more theoretical) data ownership issues (Deloitte et al., 2017).

A recent survey showed that companies that have not yet engaged in B2B (business to business) data sharing mentioned 3 main factors which would facilitate it (Benelux E., 2018): legal clarity about "data ownership rights" (62%), ability to track the usage of data (46 %) and increased certainty about the nature of and procedures related to licensing agreements (42 %). The same survey showed that, for companies reporting to have experienced obstacles to data re-use, 66 % mentioned denial of access as the main one (Benelux E., 2018); the other main obstacles mentioned included unfair (discriminating or costly) conditions of access, lack of interoperability and standardization and data localization concerns.

More particularly on public sector data, one of the start-ups insist on the following issues, which they saw as missing in terms of regulation:

- the importance of FAIR principles (Findable, Accessible, Interoperable and Re-usable) data;
- its experience that there is in general more data available as open data in a machine-readable format from the US government compared to the EU institutions (also citing European Medicines Agency (EMA) data vs. Food & Drug Administration (FDA) data);
- the fact that data from governments and public institutions should be made public as machine-readable data.

The review of the PSI Directive would contribute to addressing these concerns.

3.5 GDPR and data protection

While it was agreed not to deal with data protection in any depth in the scope of this document, one should however mention that start-ups have indeed mentioned the GDPR and data protection in relation as one of the important issues they have to deal with in the development of their activities. When dealing with personal data, it is easy to see that "mining" the data will automatically amount to "processing" it, thereby triggering the application of the GDPR. Concerns about the divergences between the Member States (MS) have been lessened by the adoption of the GDPR, but MS do still have some room for manoeuvre, and more importantly, the implementation of the GDPR by small firms requires a lot of efforts and may bring with it practical difficulties. At the same time, it is worth noting that some flexibility and facilitation have been foreseen for processing of personal data for scientific research purposes or also statistical purposes, but most projects could not benefit from this category (Triaille J.P., 2018).

What comes out of the questionnaire by EIT and JRC?

They fear that *"the growing concerns about data privacy hamper the use of public open data" and that the GDPR "should be interpreted in a reasonable and flexible way in order to effectively conciliate the need to protect personal data and the data-oriented activities of start-ups (...)".*

At the same time, they acknowledge that the GDPR can at the same time also be a *"business opportunity"* or that, even if it entailed additional work or costs, *"compliance with the regulatory framework helps build trust in our business model"*.

CONCLUSIONS

The project has highlighted many areas where technological development has left current laws and regulations behind in almost all jurisdictions and therefore, in order to provide some certainty as to what is 'safe' and what is 'acceptable', the CAV industry, e-health providers and data aggregators, users and repositories need to work more closely with lawyers and regulators to formulate acceptable rules that both keeps the consumer safe and at the same time enables the AI innovators to develop and thrive. Regulators without an understanding of the technological issues will find it hard to produce legislation that is relevant, useful and able to meet the requirements outlined above and so it is beholden upon them to use industry experts to help. The AI industry is a rapidly developing and maturing industry that will have a profound impact upon most of society. The challenges for legislators and regulators is to ensure that existing rules encourage and foster innovation rather than impede it and that new laws and standards are developed to deal with any ambiguity or gaps in the existing legislative framework. These will need to be examined on a sector-by-sector basis and so will require a great deal of analysis.

Acknowledgements

Special thanks to all the EIT supported start ups that have contributed to this research as well as to the speakers and participants of the workshop, to our colleagues from the EIT and to Amanda Arenberg and to Marine Tabory whose support has been crucial for the success of the project.

FOOTNOTES

[1] As a follow up of the later the EC has launched a public consultation aiming at identifying “from the general public and relevant stakeholders the main challenges linked to the deployment of connected and automated cars today”, vid. https://ec.europa.eu/info/consultations/public-consultation-recommendation-connected-and-automated-mobility-cameramen

[2] All presentations from the workshop are available to the public on the event webpage: https://ec.europa.eu/jrc/en/event/workshop/legal-and-regulatory-implications-artificial-intelligence-ai

[3] The AI on Demand Platform was launched few weeks after the Workshop took place on January 2019, more info on https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-ai4eu-project-launches-1-january-2019. As highlighted by Ms Huet, the platform aims at becoming the central access point, integrating tools and resources and offering solutions and support to all users of AI to integrate such technology into application, products and services

[4] More information on Digital Innovation Hubs see: https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs

[5] Notably through the European Innovation Council (EIC) pilot and through the European Fund for Strategic Investments.

[6] More information on the High Level Expert Group on Artificial Intelligence see: https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

[7] More information on the European AI Alliance see: https://ec.europa.eu/digital-single-market/en/european-ai-alliance.

[8] Directive (EU) No 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

[9] More information on Algorithm Awareness Building pilot’s website: https://www.algoaware.eu/

[10] The flagship report combines effort from 11 units of the JRC and aims at giving a balanced assessment of opportunities and challenges of AI from an EU perspective, and supporting the development of European actions in the global AI context. In a nutshell the following messages come out from the report : (1) AI is a big opportunity to improve our lives and shape the future, (2) No EU Member State can succeed alone, (3) solutions need to be based on European values, (4) Computing and data is of crucial importance (5) ethical and inclusive by design has to be reached, (6) the EU should build on European areas of strength – robotics, connected & automated vehicles.

[11] More information on the AI Watch page: https://ec.europa.eu/knowledge4policy/ai-watch_en.

[12] Currently the EIT finances about 50 AI related activities (innovation or education projects and start-ups); among 5 EIT Awards winners in 2018, 3 were linked to AI.

[13] See in particular the MS declaration of cooperation Towards access to at least 1 million sequenced genomes in the European Union by 2022

[14] More info on the Code of conduct on privacy in mHealth, see: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

[15] The EC Communication highlights technical and legal issues and addresses three sectors: public, private and research. The 2018 Data Package specifies that each sector will have a different set of policy instruments comprising of a mix of laws, recommendations and/or guidelines. The Data Package includes one evaluation and two communications.

[16] The common vision now focuses on automation levels 3 to 4, which entails going from the driver not having to monitor the system at all times but must always be in position to resume control, to the driver not being required during defined use.

[17] Here, different legal texts and ongoing initiatives can be mentioned: in addition to the vehicle and traffic rules; the EU motor Insurance Directive for quick victim compensation; the Product Liability Directive for manufacturer responsibility; as well as the work carried out by the EC Expert Group on liability and new technologies. A recent public consultation also highlights the relevance of data governance and privacy issues for the future of connected and autonomous services; see Public consultation on Recommendation on Connected and Automated Mobility (CAM), more info available

on *https://ec.europa.eu/info/consultations/public-consultation-recommendation-connected-and-automated-mobility-cam_en*.

18 The EU has made significant investments on automated road transport through H2020 and the H2020 – Calls on "Automated Road Transport". 300 million have been allocated for 2014-2020 with precise focuses: Large-scale demos of automated driving systems for passenger cars, trucks and urban transport; Safety and end user acceptance; Road infrastructure to support automation; Traffic management solutions; Connectivity for automation; Testing and validation procedures; Assessment of impacts, benefits and costs of CAD systems; Support for cooperation and networking activities; Human centered design of AV. Two calls will open in 2019: Human centered design for the new driver role in highly automated vehicles; and Developing and testing shared, connected and cooperative automated vehicle fleets in urban areas for the mobility of all. Two calls will also open in 2020: Efficient and safe connected and automated heavy commercial vehicles in real logistics operations and Large-scale, cross-border demonstration of highly automated driving functions for passenger cars

19 The key novelties will be a European Innovation Council, R&I missions, extended association possibilities, open science policy, new approach to partnerships. The three pillars will be: open science, global challenges and open innovation.

20 Jean Francois Aguinaga, Head of Surface Transport Unit, Director – General for Research and Innovation, European Commission.

21 For an overview on legal issues and AI, see: de Streel, A & Jacquemin, H., (eds.), L'intelligence artificielle et le droit, Brussels, Larcier, Collection du Crids, 2017 ; see also Poullet, Y., Le droit face aux développements de l'intelligence artificielle dans le domaine de la sant », Revue Lamy Droit de l'immatériel, 2018, n°152, p.43 - 52

22 See European Data Protection Supervisor, Mobile Health: reconciling technological innovation with data protection (opinion 1/2015), *https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf*

23 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR*

24 As indicated by art. 4, (5) GDPR, "pseudonymisation" means "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." The limit between anonymous and pseudonymous data in e-health might be confused. This raises another question: is the anonymization of health related data feasible?

25 Recital 39 of the GDPR.

26 See also Delforge, A., Les droits de la personne concernée dans le RGPD, Le Règlement général sur la protection des données (RGPD / GDPR), Collection du Crids, 2018, pp. 407-432.

27 AI environment means any application, software involving AI in its processing.

28 Articles 12 to 14 GDPR.

29 This means that, as a general rule rule, the patient must consent before any intervention of a health practitioner (except, of course, in case of an emergency). See Jones V., Jolli C., eHealth strategy and implementation activities in England, report in the framework of the eHealth ERA project, June 7th 2007, *http://ehealth-strategies.eu/database/documents/England_eHealth_ERA_country_report.pdf*; *www.nhs.uk/conditions/consent-to-treatment/*; French Code of ethics, article 36, *www.conseil-national.medecin.fr/article/article-36-consentement-du-malade-260*; Le Goues, M. Le consentement du patient en droit de la santé, Thèse en droit, Université d'Avignon, 2015, *https://hal.archives-ouvertes.fr/hal-00872135*; Brosset, E., Le consentement en matière de santé et le droit européen, 2013, *https://hal.archives-ouvertes.fr/hal-00872135*

30 On the notion of consent, see: Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01, April 10th, 2018.

31 We also observe that there may be other issues are not related to the GDPR contrary of what could think of. For example, the European Union does not have exclusive powers regarding the Health sector. Each Member State has its own legislation, which implies implementation issues specific to each country. Therefor the GDPR is not the cause of a lack of harmonisation in health law.

32 This refers to the multi-factor authentication meaning that access to the program or data is granted only after having successfully presented two or more pieces of evidence (e.g. password with answer to a personal question).

33 Article 20 of the GDPR and Recital 68 of the GDPR.

34 Article 29 Working Party, Guidelines on the right to data portability, 13.12.2016, p. 4.

35 Article 29 Working Party, Guidelines on the right to data portability, 13.12.2016, p. 9. But the right of access (and the possibility to receive a copy) may apply.

36 Article 29 Working Party, Guidelines on the right to data portability, 13.12.2016, p. 8.

37 Article 25, 1 of the GDPR.

38 Ibidem.

39 Ibidem.

40 The Article 29 Working Party indirectly tackles this aspect between product provider and data controller in the Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, p. 8.

41 Article 28, 1 GDPR.

42 Article 9, (1) Regulation 2017/745.

43 Article 2, (1) Regulation 2017/745.

44 Article 2, (1) Regulation 2017/745.

45 Recital 2 Regulation 2017/745; we underline.

46 See European Court of Justice, Syndicat national de l'industrie des technologies médicales (Snitem) and Philips France v Premier ministre and Ministre des Affaires sociales et de la Santé (C-329/16), 7.12.2017, #21 and following ; Ronneau, V., La Responsabilité civile en matière de dispositifs médicaux: évolutions récentes, Le droit des machintechs (FinTech, LegalTech, MedTech…): états des lieux et perspectives, Bruxelles, Larcier, p. 185.

47 As noted in the Green paper on m-Health, in the US “the Food and Drug Administration (FDA) published in September 2013 a Guidance on Mobile Medical Applications to inform app manufacturers and distributors about how it intends to apply its regulatory authority to apps intended for use on mobile platforms. The FDA approach calls for oversight of only those mobile apps that are medical devices and whose functionality could pose a risk to a patients' safety if the app does not function as intended” .In the European Union, we have a similar document clarifying “the distinction between different types of medical software” (*https://ec.europa.eu/docsroom/documents/17921/attachments/1/translations/en/renditions/native*)

48 See, amongst others, article 13 Regulation 20187/745.

49 The issue is tackled by both legal doctrine and jurisprudence.

50 Even if the GDPR do not handle this, the Article 29 working party (European Data Protection Board since May 25th 2018) dealt this in “Guidelines on Data Protection Impact Assessment (DPIA)” available at: *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*

51 See article 9, 2, j and article 89 of GDPR.

52 ‘Healthcare’ means health services provided by health professionals to patients to assess, maintain or restore their state of health, including the prescription, dispensation and provision of medicinal products and medical devices. (Article 3, (a) Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients’ rights in cross-border healthcare)

53 E.g., a letter to the Commission and entitled Maximising the benefits of Artificial Intelligence through future-proof rules on Text and Data Mining, dd. 9 April 2018, refers to the "foundational role that Text and Data Mining plays in AI" and describes it as "a building block for both machine and deep learning"; available at *http://eare.eu/assets/uploads/2018/03/OpenLetter-to-European-Commission-on-AI-and-TDM_9April2018.pdf*

54 The proposed amendment reads as follows: *"Without prejudice to Article 3 of this Directive, Member States may provide for an exception or a limitation to the rights provided for in Article 2 of Directive 2001/29/EC, Articles 5(a) and 7(1) of Directive 96/9/EC and Article 11(1) of this Directive for reproductions and extractions of lawfully accessible works and other subject-matter that form a part of the process of text and data mining, provided that the use of works and other subject*

matter referred to therein has not been expressly reserved by their rightholders, including by machine readable means."

[55] For an overview of the academic discussion in a number of European countries (France, Germany, UK, Spain).

[56] *"(...) policy solutions in regard to access to privately held data, and particularly obligations to grant access, will need very careful consideration and justifications."*

[57] See also on the different possible modalities of a non-consensual right of access.

[58] See for instance the Payment services Directive II, Regulation 715/2007, etc.

REFERENCES

Baker McKenzie, Global driverless vehicle survey, 2018. *https://www.bakermckenzie.com/-/media/files/insight/publications/2018/03/global-driverless-vehicle-survey-2018/mm_global_driverlessvehiclesurvey2018_mar2018.pdf*

Benelux E., Study on data sharing between companies in Europe, Study prepared for DG CNECT, 2018

Brosset E., Le consentement en matière de santé et le droit européen, 2013. *https://hal.archives-ouvertes.fr/hal-00872135*

BSI and the Transport Systems Catapult, Connected and autonomous vehicles, A UK standards strategy, Summary report, 2017. *https://s3-eu-west-1.amazonaws.com/media.ts.catapult/wp-content/uploads/2016/03/23141343/CAV-standards-strategy-summary-report.pdf*

Butcher L. & Edmonds T., Briefing paper: the Automated and Electric Vehicles Act 2018, House of Commons Library, 2018. *http://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf*

Craglia M. (Ed.), Annoni A., Benczur P., Bertoldi P., Delipetrev P., De Prato G., Feijoo C., Fernandez Macias E., Gomez E., Iglesias M., Junklewitz H, López Cobo M., Martens B., Nascimento S., Nativi S., Polvora A., Sanchez I., Tolan S., Tuomi I., Vesnic Alujevic L., Artificial Intelligence - A European Perspective, EUR 29425 EN, Publications Office, Luxembourg, 2018, ISBN 978-92-79-97217-1, doi:10.2760/11251, JRC113826.

De Streel A & Jacquemin, H., (eds.), L'intelligence artificielle et le droit, Brussels, Larcier, Collection du Crids, 2017

Delforge A., Les droits de la personne concernée dans le RGPD, Le Règlement général sur la protection des données (RGPD / GDPR), Collection du Crids, 2018, pp. 407-432.

Deloitte et al., Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability, Study prepared for DG CNECT, 2017

Duch-brown N., Martens B. & Mueller-langer F., The economics of ownership, access and trade in digital data, JRC Technical Reports, 2017

Dumortier F., La sécurité des traitements de données à caractère personnel, Le Règlement général sur la protection des données (RGPD / GDPR), Collection du Crids, 2018, pp. 141-252

European Commission (EC) 2016. Proposal for a Directive of the European Parliament and of the council on copyright in the Digital Single Market, COM(2016)593 final Brussels.

European Commission (EC) 2017. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. *http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236*

European Commission (EC) 2018a. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe, COM(2018)232 final Brussels.

European Commission (EC) 2018b. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018)233 Brussels.

European Commission (EC) 2018c. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the road to automated mobility: An EU strategy for mobility of the future COM(2018)283 final Brussels.

European Commission (EC) 2018d. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe COM(2018)237 final Brussels.

European Commission (EC) 2018e. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Towards a common European Data space COM(2018)232 final Brussels.

European Commission (EC) 2018f. Proposal for a Regulation of the European Parliament and of the Council establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination,(COD) 2018/0224 Brussels.

European Commission (EC) 2018g. Commission staff working document, Liability for emerging digital technologies SWD(2018) 137 final Brussels

European Commission (EC) 2018h. Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information.

European Commission (EC) 2018i. Commission staff working document, Guidance on sharing private sector data in the European data Economy SWD(2018)125 final Brussels.

European Commission (EC) 2018j. Proposal for A Directive Of The European Parliament And Of The Council on the re-use of public sector information (recast) COM(2018) 234 final Brussels

European Commission (EC) 2018k., Proposal for a Regulation of the European Parliament and of the Council on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/... and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009, COM/2018/286 final - 2018/0145 (COD)

European Data Protection Supervisor (EDPS) 2015. Mobile Health: reconciling technological innovation with data protection (opinion 1/2015), https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf

European Parliament (EP) 2016. Report on the proposal for a directive of the European Parliament and of the Council on copyright in the Digital Single Market (COM(2016)0593 – C8 0383/2016 – 2016/0280(COD)).

European Parliament (EP) 2018. Research Service's study on A common EU approach to liability rules and insurance for connected and autonomous vehicles. *http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf*

Evas T., European Parliamentary Research Service's study, A common EU approach to liability rules and insurance for connected and autonomous vehicles, 2018. http://www.europarl.europa.eu/RegData/etudes/STUD/2018/615635/EPRS_STU(2018)615635_EN.pdf

Federation Internationale de l'Automobile, What EU legislation says about car data - Legal Memorandum on connected vehicles and data, 2017. http://www.osborneclarke.com/wp-content/uploads/2017/08/OSB100213_FIA-Car-Data-Report_v1.pdf
Ferrara S.D. & Baccino E., and alii, Malpractice and medical liability, European Guidelines on Methods of Ascertainment and Criteria of Evaluation, 2013. https://www.uems.eu/__data/assets/pdf_file/0005/19616/Item-3.2.7-European_Medico_legal_Guidelines.pdf

Freshfields Bruckhaus Deringer, Automated driving law passed in Germany, 2017. https://www.freshfields.com/en-gb/our-thinking/campaigns/digital/internet-of-things/connected-cars/automated-driving-law-passed-in-germany/
Geiger C., Frosio G. & Bulayenko O., The Exception for Text and Data Mining (TDM) in the Proposed Directive on Copyright in the Digital Single Market – Legal Aspects, 2018. http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/604941/IPOL_IDA(2018)604941_EN.pdf

Graef I., Husovec M. & Purtova N., Data Portability and Data Control: Lessons for an Emerging Concept in EU Law, December 15, 2017, TILEC Discussion Paper No. 2017-041; Tilburg Law School Research Paper No. 2017/22. Available at SSRN: https://ssrn.com/abstract=3071875 or http://dx.doi.org/10.2139/ssrn.3071875

Graf von Westphalen F., The End of the Traditional Contract Concept, in Lohsse S., Schulze, R. & Staudenmayer D., (eds), Trading Data in the Digital Economy: Legal Concepts and Tools, Hart Publishing/Nomos, 2017

Hargreaves I., et al., Report from the Expert Group, Standardisation in the area of innovation and technological development, notably in the field of text and data mining, 2014. http://ec.europa.eu/research/innovation-union/pdf/TDM-report_from_the_expert_group-042014.pdf

Hatipoglu C., US NHTSA's non-binding guidance: Cyber Security Best Practice for Modern Vehicles, 2016. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/sae2017chatipoglu_0.pdf

International Conference of Data Protection & Privacy Commissioners, Declaration on Ethics and Data Protection in Artificial Intelligence, 2018a. https://icdppc.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

International Conference of Data Protection & Privacy Commissioners, Public consultation, 2018b. https://icdppc.org/public-consultation-ethics-and-data-protection-in-artificial-intelligence-continuing-the-debate/

International Organization for Standardization, ISO/TC 204 Intelligent Transport systems. https://www.iso.org/committee/54706.html

Jondet N., L'exception pour le data mining dans le projet de directive sur le droit d'auteur, Propriétés Intellectuelles, n° 67, april 2018

Jones V., Jolli C., eHealth strategy and implementation activities in England, report in the framework of the eHealth ERA project, June 7th 2007. http://ehealth-strategies.eu/database/documents/England_eHealth_ERA_country_report.pdf

Kerber W., A New (Intellectual) Property Right for Non-Personal Data? An Economic Analysis, GRUR Int., 2016

Kerber W., Rights on data: the EU Communication 'Building a European Data Economy' from an Economic Perspective, in Lohsse

S., Schulze R. & Staudenmayer D., (eds), Trading Data in the Digital Economy: Legal Concepts and Tools, Hart Publishing/Nomos, 2017

KWM, Self-driving Cars: Who will be Liable?, 2017. *https://www.kwm.com/en/knowledge/insights/self-driving-cars-who-will-be-liable-20170829*

Le Goues M., Le consentement du patient en droit de la santé, Thèse en droit, Université d'Avignon, 2015. *https://hal.archives-ouvertes.fr/hal-00872135*

Mezzanotte F., Access to Data: the Role of Consent and the Licensing Scheme, in Lohsse S., Schulze R. & Staudenmayer D., (eds), Trading Data in the Digital Economy: Legal Concepts and Tools, NOMOS, 2018

Norton Rose Fulbright, Autonomous vehicles: The legal landscape of DSRC in the United Kingdom, 2017. *http://www.nortonrosefulbright.com/knowledge/publications/154715/autonomous-vehicles-the-legal-landscape-of-dsrc-in-the-united-kingdom*
Osborne C., Legal study on ownership and access to data, Final report – Study, 2016 *https://publications.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1*

Peng T., Global Survey of Autonomous Vehicle Regulations, AI Technology & Industry Review, 2018. *https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9*

Pinsent Masons, Connected and Autonomous Vehicles: The emerging legal challenges, 2016. *https://www.pinsentmasons.com/PDF/2016/connected-and-autonomous-vehicles-2016.pdf*

Poullet Y., Le droit face aux développements de l'intelligence artificielle dans le domaine de la santé, Revue Lamy Droit de l'immatériel, 2018, n°152, p.43 - 52

Ronneau V., La Responsabilité civile en matière de dispositifs médicaux: évolutions récentes, Le droit des machintechs (FinTech, LegalTech, MedTech…): états des lieux et perspectives, Bruxelles, Larcier, 2018, p. 181-222.

Schellekens M., No-fault compensation schemes for self-driving vehicles, Law, Innovation and Technology, 2018. DOI: 10.1080/17579961.2018.1527477

The European Data Market, Final report, February 2017, SMART 2013/0063, *http://datalandscape.eu/study-reports*

Triaille J.P., Meeus J., De Francquen A., Study on the legal framework of text and data mining (TDM), March 2014. *https://publications.europa.eu/en/publication-detail/-/publication/074ddf78-01e9-4a1d-9895-65290705e2a5/language-en*

Triaille J.P., The exception for scientific research under EU copyright law and EU privacy law, in Poullet, Y., Laws, Norms and Freedoms in Cyberspace – Droits, normes et libertés dans le cybermonde, Liber amicorum, Larcier, 2018.

United Kingdom, Automated and Electric Vehicles Act, 2018. *http://www.legislation.gov.uk/ukpga/2018/18/contents/enacted*

United Kingdom, Consumer Protection Act, 1987. *https://www.legislation.gov.uk/ukpga/1987/43/contents*

United Kingdom, Department of Transport, The key principles of vehicle cyber security for connected and automated vehicles, 2017. *https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles*

United Kingdom, Privacy and Electronic Communication (EC Directive) Regulations, 2003. *http://www.legislation.gov.uk/uksi/2003/2426/contents/made*

US Department of Transport, Comprehensive Management Plan for Automated Vehicle Initiatives, 2018. *https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/317351/usdot-comprehensive-management-plan-automated-vehicle-initiatives.pdf*

US Department of Transportation, US National Highway Transportation Safety Administration, Guidelines: Automated Driving Systems 2.0: Vision for Safety, 2017. *https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf*

Van Gyseghem J.-M., The Belgian Digital Health Valley: enabling patient contributions to healthcare, Digital Health Legal, 3:10, 2016, pp. 12-13.

Wessing T., Driverless cars and product liability, 2017. *https://www.taylorwessing.com/download/article-driverless-cars-and-product-liability.html*

KJ-04-19-359-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/527052
ISBN 978-92-76-02040-0