Ethical and legal challenges of artificial intelligence-driven healthcare

Week 4

Liability

The NTF's findings include that
liability regimes
are mainly **regulated by the EU Member States**,
except for
strict liability of producers for defective products,
that is **regulated by the Product Liability Directive at the EU level**.

The NTF's opinion is that
the Member States' liability regimes
are a good starting point for new technologies and provide at least basic protection of victims.

However, **the NTF also identifies several points that need to be changed at national and EU levels**.

For example,
the NTF emphasizes that
a person operating a permissible technology that nevertheless carries an increased risk of harm to others, for example AI-driven robots in public spaces,
should be subject to strict liability for damage resulting from its operation.

Liability

It also states, for instance, that
a person using a technology which has a certain degree of autonomy should not be less accountable for ensuing harm than if said harm had been caused by a human auxiliary.

In February 2020,
the European Commission also published a report on
the safety and liability implications of AI, the IoT, and robotics.

The European Commission understands the importance of these technologies and aims to make "Europe a world-leader in AI, IoT, and robotics".

To achieve this aim,
the European Commission states that
"a clear and predictable legal framework addressing the technological challenges is required".

The European Commission,
in accordance with the NTF,
argues that
"in principle the existing liability laws are able to cope with emerging technologies".

Liability

However,
it also identifies some challenges raised by new digital technologies
such as AI
that need to be addressed
by adjustments in the current national and EU regulatory frameworks
such as the Product Liability Directive.

Data protection and privacy

United States

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (45 C.F.R. Part 160 as well as subparts A and E of Part 164)
is the key federal law
to protect health data privacy.

However,
HIPAA has significant gaps
since it only covers specific health information
generated by "covered entities" or their "business associates."

HIPAA
does not apply to nonhealth information that supports inferences about health
such as a purchase of a pregnancy test on Amazon.

Data protection and privacy

United States

The definition of "covered entities" includes insurance companies, insurance services, insurance organizations, healthcare clearinghouses, and healthcare providers (45 C.F.R. yy 160.102, 160.103).

Amazon, Google, IBM, Facebook, and Apple are not "covered entities," and **will fall outside** of HIPAA.

HIPAA **does not apply** in cases of user-generated health information.

For example, a Facebook post about a disease **falls outside** of HIPAA's regime.

Data protection and privacy

United States

A different problem with HIPAA is its reliance on de-identification as a privacy strategy.

Under HIPAA, de-identified health information can be shared freely for research and commercial purposes [45 C.F. R. y 164.502(d)(2)].

It provides **two options** for de-identification:

(1) a determination by someone with appropriate knowledge of and experience with usually accepted scientific and statistical methods and principles; or

(2) the removal of 18 identifies (e.g., names, social security numbers, and biometric identifiers) of the individual or of relatives, household members, or employers of the individual, and no actual knowledge of the covered entity that the information could be used to identify an individual [45 C. F.R. y 164.514(b)].

Data protection and privacy

United States

This
may not adequately protect patients
because of
the possibility of data triangulation to re-identify data
althought to be de-identified through the combination of multiple datasets.

The problem of data triangulation has been featured in a lawsuit,
Dinerstein v. Google,
in which
the plaintiffs alleged that
the defendants shared medical records with Google
containing enough information
that enabled Google to potentially re-identify patients
given all of its other data at hand.

Data protection and privacy

United States

For all these reasons,
HIPAA is not adequate to protect the health privacy of patients.

It is time for federal law
to take seriously
the protection of health-relevant data
that is not covered by HIPAA.

Such a federal law
should facilitate
both innovations, including health AI applications, and adequate protection of health privacy of individuals.

Inspired by the EU GDPR,
California has taken action at the state level: The California Consumer Privacy Act of 2018 (CCPA) became effective on January 1, 2020 (Cal. Civ. Code y 1798.198).

Data protection and privacy

Europe

The General Data Protection Regulation (GDPR–2016/679) has been applied since May 25, 2018 [Art. 99(2) of the GDPR] in all EU Member States and introduced a new era of data protection law in the EU.

The GDPR **aims** to protect the right of natural persons to the protection of personal data [Art. 1(2) of the GDPR].

It applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the EU, **notwithstanding of whether the processing takes place in an EU or non-EU country**, such as in the US [Arts. 2, 3(1) of the GDPR].

Data protection and privacy

Europe

The GDPR may also have implications for US companies.

For example,
the Regulation **applies** in cases where
the processor or controller
is established in a non-EU country and
processes personal data of data subjects who are in the Union

- for the offering of goods or services (e.g., newspapers and affiliated websites for free or for a fee) to such data subject in the EU, or
- for the monitoring of the data subjects' behavior [Art. 3(2) of the GDPR]

The GDPR
also **applies** where
a controller
processes personal data and
is established in a non-EU country,
but in a place where Member State law applies by virtue of public international law
[Art. 3(3) of the GDPR]

Data protection and privacy

Europe

The GDPR defines

- *"personal data" as any information relating to an identified or identifiable natural person ('data subject') [Art. 4(1) of the GDPR].*
- *"processing" as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, including collection, structuring, storage, or use [Art. 4(2) of the GDPR].*
- *a "controller" as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*
- *a "processor" as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller [Arts. 4(7), (8) of the GDPR].*

Data protection and privacy

Europe

In the healthcare context,
the definition of "data concerning health" under Article 4(15) of the GDPR includes personal **data related to the physical or mental health of a natural person, including the provision of healthcare services**, which reveal information about his or her health status.

The EU's GDPR
is a lot broader in its scope compared to US' HIPAA,
which only covers specific health information generated by "covered entities" or their "business associates".

According to Article 9(1) of the GDPR,
the processing of **special categories** of personal data
such as

- genetic data [Art. 4(13) of the GDPR],
- biometric data [Art. 4(14) of the GDPR], and
- data concerning health

is prohibited.

Data protection and privacy

Europe

Article 9(2) of the GDPR
contains a **list of exceptions** to paragraph 1.

For example,
the prohibition in Article 9(1) of the GDPR
shall usually **not apply** in cases where

- the data subject has given explicit consent (...) for one or more specified purposes, or
- the processing is necessary
    - for reasons of public interest in the area of public health, or
    - for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes [Art. 9(2)(a), (i), and (j) of the GDPR]

The EU Member States
can decide to introduce or maintain further requirements, including limitations,
but only with regard to the processing of **genetic data, biometric data or data concerning health** [Art. 9(4) of the GDPR].

Data protection and privacy

Europe

Noncompliance with these GDPR's conditions
will result in administrative fines up to 20 million EUR or up to 4% of an undertaking's annual global turnover of the previous year [Art. 83(5) of the GDPR].

The first fines in the healthcare context have already been imposed under the GDPR.

For example,
a hospital in Portugal was charged 400 thousand EUR for two breaches of the GDPR: First, 300 thousand EUR for the permit of "indiscriminate access to a set of data by professionals, who should only be able to access them in specific cases"; and second, 100 thousand EUR for the incapacity to "ensure the confidentiality, integrity, availability and permanent resilience of treatment systems and services".

Data protection and privacy

Europe

The GDPR also contains provisions that are especially relevant to medicine.

For example,
where personal data are collected,
the controllers must generally provide data subjects with information about the existence of ***automated decision-making****, including profiling, referred to in Article 22(1) and (4) and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject [Arts. 13(2)(f), 14(2) (g) of the GDPR].*

In addition,
data subjects have the right of access to the personal data concerning them that are being processed and the information about "the existence of automated decision-making, including profiling, (...) and (...) meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject" [Art. 15(1)(h) of the GDPR].

Data protection and privacy

Europe

Definitions:

- *"Automated decision-making": a decision that is made—without any human involvement—solely by automated means.*

- *"profiling": any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.*

Thus the term "profiling" is a subset of the term "processing" with two additional requirements: the processing must be (1) automated and (2) for evaluation purposes.

Under Article 22(1) of the GDPR,
data subjects shall also have the right not to be subject to a decision based solely on automated processing, including profiling."

Article 22(2) of the GDPR
lists some exceptions to Article 22(1) of the GDPR,
but these exceptions do generally not apply where decisions are based on genetic and biometric data as well data concerning health [Art. 22(4) of the GDPR].

Data protection and privacy

Europe

It is highly controversial,
whether the GDPR actually grants a "right to explanation" and what such a right means.

Recital 71 of the GDPR explicitly mentions "the right (...) to obtain an explanation of the decision reached after such assessment."

Some scholars doubt the legal existence of such a right to explanation of specific automated decisions,
because a right to explanation is not mandated by the legally binding requirements set out in Article 22(3) of the GDPR.

Thus, according to this view,
there is no legally binding right of the data subject to receive insight into the internal decision-making process of algorithms, and thus to open the "black boxes" of health AI applications.

Data protection and privacy

Europe

However,
if a legally binding right to explanation of specific automated decisions does not exist,
Articles 13(2)(f), 14(2)(g), and 15(1)(h) of the GDPR
at least entitle data subjects to obtain meaningful information
about the logic involved, as well as the significance and the consequences of automated decision-making systems.

This information includes

- the purpose of an automated decision-making system,
- how the system works in general,
- the predicted impact and,
- other system functionality such as decision trees and classification structures

It is also likely that
companies that are controllers under the GDPR
must carry out
a data protection impact assessment
for new AI-based technologies that shall be deployed in the clinical space.

Data protection and privacy

Europe

Article 35 (1) of the GDPR requires such an assessment,
prior to the processing,
for new technologies where the processing is likely to result in a high risk to the rights and freedoms of natural persons.

Article 35(3) of the GDPR explicitly states when a data protection impact assessment shall especially be required.

Article 35(7) of the GDPR contains a list of what the assessment shall at least include,
such as

- *a description of the envisaged processing operations,*
- *an assessment of the risks to the freedoms and rights of data subjects, and*
- *the measures envisaged to address the risks*

As complementation to the GDPR,
the Regulation (EU) 2018/1807 entered into force in December 2018 and has been directly applicable since May 28, 2019 (Art. 9 of Regulation 2018/1807).

This Regulation
contains a framework
for the free flow of nonpersonal data in the EU
(Art. 1 of Regulation 2018/1807).

Data protection and privacy

Europe

It **applies**
to the processing of electronic data [other than personal data as defined in Art. 4(1) of the GDPR] in the EU,
which is either

- provided as a service to users residing or having an establishment in the Union,

irrespective of whether the service provider is established in an EU or non-EU country,
or

- carried out by a natural or legal person residing or having an establishment in the Union for its own needs

[Arts. 2(1), 3(1) and (2) of Regulation 2018/1807]

In cases of datasets composed of personal and nonpersonal data,
the Regulation (EU) 2018/1807
does also **apply**
to the nonpersonal data part of such datasets
[Art. 2(2) of Regulation 2018/1807].

However,
the GDPR
applies
in cases where the personal and nonpersonal data in datasets are inextricably linked
[Art. 3(2) of Regulation 2018/1807].

Cybersecurity

In the future,
much of the healthcare-related services, processes, and products
will operate within the IoT.

Much of the underlying infrastructure is vulnerable to both ***cyber and physical threats and hazards****.*

For example, sophisticated cyber actors can exploit vulnerabilities to steal or influence the flow of money or essential (healthcare) information.

Targets in the health sector may include hospital servers, diagnostic tools, wearables, wireless smart pills, and medical devices.

Moreover, corrupted data or infected algorithms can lead to incorrect and unsafe treatment recommendations.

Hostile actors could get access to sensitive data such as health information on patients or could threaten patients' safety by misrepresenting their health.

AIs are vulnerable to manipulation.

For example,
the need for increased cybersecurity was shown in a global cyberattack using sophisticated hacking tools that crippled the National Health Service (NHS) in the UK.

Cybersecurity

Events like these
not only resulted in reactions at the national level such as in the UK
but also prompted a new Cybersecurity Act [Regulation (EU) 2019/881]
that came into force on June 28, 2019.

The new Cybersecurity Act's goals are to achieve a high level of cyber resilience, cybersecurity, and trust in the EU while ensuring the internal market's proper functioning [Art. 1(1)].

The Act,

- *lays down a European cybersecurity certification framework to ensure that certified information and communications technology (ICT) products, ICT services, and ICT processes in the EU fulfill an adequate level of cybersecurity [Art. 1 (1)(b)]*
- *lays down the tasks, objectives, and organizational matter relating to the European Union Agency for Cybersecurity (ENISA) [Art. (1)(a)].*

There is also new progress in the US:
The Cybersecurity and Infrastructure Security Act of 2018 (H.R.3359) was signed into law by President Donald Trump on November 16, 2018 [107].

Cybersecurity

This Act (Sec. 2)
redesignated
the National Protection and Programs Directorate of the Department of Homeland Security
as
the Cybersecurity and Infrastructure Security Agency (CISA)
(Sec. 2202; 6 U.S.C. 652).

CISA

- augments the US national capacity to defend against cyberattacks and
- helps the federal government provide cybersecurity tools, assessment skills, and incident response services to safeguard sensitive networks

While the latest legal developments in the US and Europe
will hopefully promote the safety of AI-driven products, services, and processes in the healthcare sector,
cyberattacks are often a global issue;
data sharing and breaches frequently do not stop at the US or European borders but occur around the world.

Thus
there is the need for an internationally enforceable, large-scale regulatory framework on cybersecurity that ensures a high level of cybersecurity and resilience across borders.

Intellectual property law

Translating
AI and big data
into safe and effective "real-world" products, services, and processes
is an expensive and risky venture.

There are continuing discussions about open science and innovation and the primary objective of more data sharing as well as increasing debates over access to such technologies and the pertinent data.

AI and the data that fuels it
can be protected by various intellectual property rights (IPRs),
typically involving a combination of

- *long contracts,*
- *copyright,*
- *trade secrets/the law of confidence,*
- *database rights, and*
- *personal data integrity rights*

The result is that data are frequently the subject of litigation.

Thus it has been suggested that more regulations for data-generating internet giants are necessary.

Intellectual property law

The combination of big data and IPRs creates challenges that need to be addressed such as access to data and ownership rights.

In cases of data mining and data analytics, various forms of IPRs might protect copying of databases and information.

However, users will need to rely on an exemption to IPR infringement where data is not licensed or owned.

This circumstance has led to disputes between data scientists and data "owners" .

Moreover, in the context of big data applications, there is a lot of misunderstanding about the nature, the availability, and legal effects of overlapping rights and remedies.

For example, copyrights might protect the software that helps to collect and process big datasets. However, due to the somewhat unstructured nature of the nonrelational databases, the traditional role and purpose of copyrights and the EU's right in databases have been called into question.

With regard to patents, recent case law in Europe (e.g., the German

Intellectual property law

With regard to patents,
recent case law in

- *Europe (e.g., the German Federal Supreme court case on receptor tyrosine kinase and the UK Illumina case) and*
- *US (e.g., the landmark cases Mayo, Myriad, and Alice)*

might have an impact on precision medicine with its aim to better tailoring treatment to the need of patients in 3 áreas:
(1) biomarkers and nature-based products,
(2) diagnostics, and
(3) algorithms, big data, and AI

- *In the US,*

recent patent law decisions made it harder to obtain patent protection for precision medicine inventions,
whereas

- *In Europe,*

a less stringent standard of patent eligibility is applied such as for nature-based biomarkers

Drug companies will most likely use AI systems to expand their traditional drug patent portfolio.

Intellectual property law

However,
AI systems
could also be used by competitors or patent examiners

- *to predict incremental innovation, or*
- *to reveal that a patent was ineligible for patent protection due to, for example, the lack of novelty or inventive step*

Furthermore, trade secret law, in combination with technological protection measures and contracts, can protect complex algorithms, as well as datasets and sets of insights and correlations generated by AI systems.

Some rights,
such as
copyrights and trade secrets,
are becoming more and more crucial for the commercial protection of big data.

Intellectual property law

The un/availability of such rights
could not only lead to underinvestment in some areas due to a lack of incentives
but also block effects for anticommons scenarios and open innovation in other áreas.

Furthermore,
the interaction between
IPRs and data transparency initiatives and
their possible impact on public/private partnerships or open innovation scenarios
should be clarified.

It becomes apparent that more data sharing is necessary in order to achieve the successful deployment of AIs in healthcare on a large scale.

Stakeholders such as companies, agencies, and healthcare providers need to consider

- *with whom they are going to collaborate, and*
- *what datasets under what conditions they are going to share*

Intellectual property law

Some stakeholders
are reluctant and refuse to share their data due to, for example, a lack of trust, previous spending on data quality or the protection of commercial and sensitive personal data.

To resolve these tensions,
legal frameworks
would be desirable that promote
data sharing through, for example, data sharing intermediaries and public/private partnerships, while ensuring adequate protection of data privacy.

In cases where stakeholders such as companies
act unfairly and collude to control a market where competition and access are essential for healthcare,
the hope is that
more refined competition and antitrust law tools can intervene.

Intellectual property law

To serve this role,
competition and antitrust law
will need to become more future-oriented
to better understand and predict the dynamics and developments of big data and AI in the healthcare sector.

The value of data differs and often depends on multiple factors, including its usage and uniqueness.

For instance,

- diverse data

that provides a multitude of signals
appears to be more useful and thus valuable

But

- if the data is unique and not replicable

may result in market power.