Alma Mater Studiorum – Università di Bologna
in cotutela con University of Luxembourg

DOTTORATO DI RICERCA IN

LAW, SCIENCE AND TECHNOLOGY

Ciclo XXXIII

Settore Concorsuale: 12/H3

Settore Scientifico Disciplinare: IUS/20

ETHICAL PERSPECTIVES
ON BIG DATA IN AGRI-FOOD:
OWNERSHIP AND GOVERNANCE FOR SAFETY

Presentata da: Salvatore Sapienza

Coordinatore Dottorato	**Supervisore**
Prof.ssa Monica Palmirani	**Prof.ssa Monica Palmirani**
	Co-Supervisore
	Prof. Mark David Cole

Esame finale anno 2021

PhD-FDEF-2021-007
The Faculty of Law, Economics and Finance

Department of Legal Studies

DISSERTATION

Defence held on 26/03/2021 in Bologna
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN DROIT

AND

DOTTORE DI RICERCA

IN LAW, SCIENCE AND TECHNOLOGY

by

Salvatore SAPIENZA
Born on 8 June 1993 in San Cataldo (Italy)

ETHICAL PERSPECTIVES ON BIG DATA IN AGRIFOOD: OWNERSHIP AND GOVERNANCE FOR SAFETY

Dissertation defence committee

Prof. Dr. Mark David Cole, dissertation supervisor
Professor, Université du Luxembourg

Prof. Dr. Monica Palmirani, dissertation co-supervisor
Professor, University of Bologna

Prof. Dr. Mariachiara Tallacchini, Chair
Professor, Università Cattolica di Piacenza

Prof. Dr. Paul de Hert, Vice Chair
Professor, University of Tilburg

Prof. Dr. Michał Araszkiewicz
Professor, Jagiellonian University

Abstract

Big data are reshaping the way we interact with technology, thus fostering new applications to increase the safety-assessment of foods, a critical goal in the protection of individuals' right to health and the flourishing of the food and feed market. An extraordinary amount of information, including real-time data available from multiple sources, is analysed using machine learning approaches aimed at detecting the existence or predicting the likelihood of future risks, thus reducing the inaccuracy of risk assessment. Food business operators have to share the results of these analyses when applying to place on the market certain products, whereas agri-food safety agencies (including the European Food Safety Authority) are exploring new avenues to increase the accuracy of their evaluations by processing Big data. Such an informational endowment brings with it opportunities and risks correlated to the extraction of meaningful inferences from data. However, conflicting interests and tensions among the involved entities - the industry, food safety agencies, and consumers - hinder the finding of shared methods to steer the processing of Big data in a sound, transparent and trustworthy way. Taken together, a recent reform in the EU sectoral legislation, the lack of trust in the EU food safety system proved by the recent Fitness Check of the General Food Law Regulation and the presence of a considerable number of stakeholders highlight the need of ethical contributions aimed at steering the development and the deployment of Big data applications. At the same time, general Artificial Intelligence guidelines and charters published by European Union institutions and Member States have to be discussed in light of applied contexts, including the one at stake. This thesis aims to contribute to these goals by discussing what principles should be put forward when processing Big data in the context of agri-food safety-risk assessment. The research focuses on two narrow and interviewed topics - data ownership and data governance - by evaluating how the regulatory framework addresses the challenges raised by Big data analysis in these domains. To do so, it adopts a cross-disciplinary research methodology that keeps into account both the technological advances and the policy tools adopted in the European Union, while assuming an ethical perspective when exploring potential solutions. The outcome of the project is a tentative Roadmap aimed to identify the principles to be observed when processing Big data in this domain and their possible implementations.

Being a researcher means that you are looking for research gaps. And if you no longer try to fill a research gap that exists, you are no longer a researcher.

Anonymous

Acknowledgements

Writing a doctoral thesis might be challenging. Doing it during a pandemic is even more so. I could not have done it without the support of many individuals within the academic community and outside. I am greatly indebted to my supervisors for their advice at the different stages of my research. Professor Monica Palmirani offered me her cross-disciplinary background to make me focus on the many "souls" of this thesis. Professor Marc David Cole offered constructive criticism on key parts of this dissertation to ensure that its contents matched the highest standards of research.

The LAST-JD board professors offered me precious advice for the development of my research plan during our meetings and provided the necessary background in law, technology, and ethics during class. Among them, Professor Anton Vedder provided useful comments in the final moments of the drafting of this document. Reviewers and defence commissioners devoted time to read this thesis and for that I am thankful to them. My colleagues Giorgia Bincoletto, Chantal Bomprezzi, Federico Galli and Valentina Leone supported me with frequent exchange of opinions and sincere friendship also beyond what was required to them as co-workers (especially abroad). Other PhD students inside and outside our programme - in particular, Arianna Rossi, Francesco Sovrano, Ludovica Paseri, Davide Liga, Pier Giorgio Chiara, Biagio Distefano, Francesca Gennari, Marta Taroni and the newcomers of the 36th Cycle of the LAST-JD - broadened the scope of my research horizons.

Outside from the LAST-JD circle, other people contributed to shape my research personality with constructive suggestions. The group made by Stefano Quintarelli, Francesco Corea, Claudia Giulia Ferrauto, Fabio Fossa, and Andrea Loreggia challenged my most monolithic views by means of their heterogeneous expertise. The people that I have met in California, including Margaret Hagan and Jorge Gabriel Jimenez, contributed to my achievements by providing the perfect environment for my research period at Stanford University. Even though Luxembourg does not quite resemble the Silicon Valley weather-wise, I have found the same warmth thanks to the people that I have met there, including Loren Jolly, Nicole Citeroni, Fabio Giuffrida, Giovanni Chiapponi, Lisa Urban, Carsten Ullrich and Teresa Alegra Quintel.

As mentioned, significant portions of this thesis have been written under lockdowns

due to COVID-19. Luckily, many friends and relatives have stayed close to me - even digitally, when necessary due to social distancing - during these tough times. I would kindly ask any non-Italian reader to apologise my switch to my native language to thank my friends and relatives. Even though they can read English, my guess is that they would like to read some thoughts in our common language.

Ringrazio moltissimo i miei genitori e il resto della mia famiglia per il supporto ricevuto in questi anni. Se sono arrivato a questo mio traguardo è anche grazie alla serenità che hanno saputo garantire. Tra i miei preziosi amici ringrazio Andrea (X2), Sergio, Angelo, Gabriele, Giorgio (X2), Carlo, e gli altri membri del nostro gruppo per le serate passate online, nonchè le mie (ex) vicine di casa Sofia, Silvia e Greta che mi hanno insegnato nuovamente la socialità al termine del primo lockdown. In ordine sparso ringrazio anche Giulia, Edoardo, Mattia, Alberto, Gianluca, Maddalena, Carlo, Vittorio, e tutte le altre persone che ho dimenticato, ma che si sentono ugualmente parte della mia vita e di questo progetto.

Contents

List of Figures

List of Tables

List of Acronyms

ADM	Automated Decision-Making
AI	Artificial Intelligence
ALTAI	The Assessment List on Trustworthy Artificial Intelligence
ANN	Artificial Neural Network
BfR	Bundesinstitut für Risikobewertung
BSE	Bovine Spongiform Encephalopathy
CAPI	Computer-assisted personal interview
CATI	Computer-assisted telephone interview
CJEU	Court of Justice of the European Union
CPR	Common-pool Resource
CSV	Comma-separated value
DCF	Data Collection Framework
DRM	Digital Rights Management
DTM	Document-term matrix
EC	European Community
ECJ	European Court of Justice
EFSA	European Food Safety Authority
ERI	Emerging Risk Identification
ERIS	Emerging Risk Identification System
EU	European Union
EUCFR	European Charter of Fundamental Rights
FAO	Food and Agriculture Organisation of the United Nations
FDA	Food and Drugs Administration
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GFLR	General Food Law Regulation
GLP	Good Laboratory Practice
GMO	Genetically Modified Organism
HACCP	Hazard Analysis and Critical Control Points
HIC	Human In-Command
HITL	Human In-The-Loop
HLEG	European Commission High-Level Expert Group
HOTL	Human On-The-Loop

IARC	International Agency for Research on Cancer
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICO	Information Commissioner's Office
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IMSOC	Information Processing System for Official Controls
ICT	Information & Communication Technology
IOT	Internet of Things
IPR	Intellectual Property Right
ISO	International Organization for Standardization
LoA	Level of Abstraction
MIKE	Method for an Integrated Knowledge Environment
NGO	Non-governmental organisation
NLP	Natural Language Processing
QPS	Qualified Presumption of Safety
PAN	Pesticide Action Network
OCA	Principal Component Analysis
PPP	Plant Protection Products
R&D	Research and Development
RALC	Restricted Access/Limited Control
RAR	Renewal Assessment Report
RASFF	Rapid Alert System for Food and Feed
RFID	Radio-frequency identifications
RPC	Raw-primary commodity
RRR	Reduced Rank Regression
SME	Small and Medium-sized Enterprise
SQL	Structured Query Language
SVM	Support Vector Machine
TDM	Term-document matrix
TF-IDF	Term-frequency /inverse document frequency
TFEU	Treaty of Functioning of the European Union
TRIPS	Trade Related Aspects of Intellectual Property Rights
UK	United Kingdom
WHO	World Health Organisation
WSN	Wireless Sensor Networks
XML	eXtensible Markup Language

List of Cases

- T-70/99 *Alpharma Inc. v Council of the European Union* [2002] ECR-II-03495

- T-13/99 *Pfizer Animal Health SA/NV v Council of the European Union* [2002] II-03305

- T-194/04 *Bavarian Lager v Commission* [2007] ECR II-3201

- C-39/05 *Sweden and Turco v Council* [2008] ECR-I-04723

- C-79/09 *Gowan Comércio Internacional e Serviços Lda v. Ministero della Salute* [2010] ECR I-13533

- T-545/11 *Stichting Greenpeace Nederland and PAN Europe v Commission* [2013] ECLI:EU:T:2013:523

- C-30/14 *Ryanair Ltd v PR Aviation BV* [2015] ECLI:EU:C:2015:10

- C-673/13 P *Commission v Stichting Greenpeace Nederland and PAN* Europe [2016] ECLI:EU:C:2016:889

- C-442/14 *Bayer CropScience SA-NV and Stichting De Bijenstichting v College voor de toelating van gewasbeschermingsmiddelen en biociden* [2016] ECLI:EU:C:2016:890

- C-57/16 P *ClientEarth v Commission* [2018] ECLI:EU:C:2018:660

- T-545/11 RENV *Stichting Greenpeace Nederland and PAN Europe v Commission* [2018] ECLI:EU:T:2018:817

- T-725/15 *Arysta LifeScience Netherlands BV, formerly Chemtura Netherlands*

BV, v EFSA [2018] ECLI:EU:T:2018:977

- T-716/14 *Anthony C Tweedale v European Food Safety Authority* [2019] ECLI:EU:T:2019:141

- T-329/17 *Heidi Hautala and Others v European Food Safety Authority* [2019] ECLI:EU:T:2019:142

1
Introduction

1.1 Big Data's impact on food safety: an overview of opportunities and risks

Of all the human activities, eating is one of the most necessary for our survival. Even though the longest fasting ever recorded lasted for 382 days (Stewart and Fleming, 1973), a research on hunger strikes has shown that the negative effects of starvation on muscles occur already within the first 10 days of fasting, while death takes place after 40 days from the last meal (M. Peel, 1997). According to Piantadosi, death from dehydration can occur after approximately 100 hours after the last swallow (Piantadosi, 2003). Eating belongs to a very restricted cluster of actions - like breathing or sleeping - upon which our existence heavily relies on.

In 1974, the Food and Agriculture Organisation of the United Nations (FAO) World Food Summit described food security as the commitment to ensure "availability at all times of adequate world food supplies of basic foodstuffs to sustain a steady expansion of food consumption and to offset fluctuations in production and prices". While this first definition was mainly concerned with the stability of times and prices of food supplies, a subsequent amendment included the concept of "access to food" in the definition of food security. Eventually, the mid-80s definition provided by FAO conceptualised food security as the goal to ensure "that all people at all times have both physical and economic access to the basic food that they need”

(FAO, 1983).

One may think that the stable availability and the access to sufficient food are the only necessary conditions to achieve food security, but this is not the case in reality. Accessibility to food alone might be insufficient in guaranteeing an healthy life. Following these considerations, in 1986 World Bank defined food security as “access of all people at all times to enough food for an active, healthy life”. Such teleological clarification was needed to broaden the scope of food security in order to include the reason *why* States should be committed to ensure food security, i.e. protecting citizens’ health. Within European Union (EU) Member States, where most people do not experience undernourishment (FAO, 2018), such qualitative approach to food security aimed at promoting policies that guarantee safe food has been put into real practice only after the occurrence of "food crises" (Alemanno and Gabbi, 2016).

A notable example of foodborne outbreak is the Bovine Spongiform Encephalopathy (BSE) - commonly referred to as Mad Cow disease - first reported in 1986 (Brown et al., 2001). The outbreak is considered one of the most significant and harmful food-borne epidemic of recent history in Europe. Once eradicated, the numbers describing this crisis were unforgiving: in the United Kingdom only, 180,000 cattle were infected and more than 4 million cattle were slaughtered. It is reported that 178 people died from mad cow-related disease (BBC, 2018). Similarly, the 2011 Escherichia Coli O104:H4 bacteria outbreak - as reported by the European Food Safety Authority (EFSA) - severely hit Germany and neighbouring countries, resulting in 4026 cases, of which 51 were fatal (EFSA, 2011b). Other more recent incidents - 2012 Salmonella outbreaks - are deemed to be responsible for 65,317 cases and 61 deaths in the EU (EFSA, 2014b).

Taken together, the starvation that is severely affecting several regions worldwide and the concern for food safety[1] in Western countries have produced a paradigm shift in the conceptualisation of food security. Today, its definition reflects the needs of both developing and developed countries. Following the BSE, in 1996 World Food Summit stated that food security "exists when all people, at all times, have physical and economic access to sufficient *safe* (emphasis added) and nutritious food to meet their dietary needs and food preferences for a healthy and active life".

The addition of safety as a crucial element of the notion of food security entails

[1] Throughout this study, notwithstanding the relevance of feedstuffs in food safety, foodstuffs will remain the main core of the thesis. It has to be preliminarily observed that the regulatory framework under scrutiny includes food- and feedstuffs within the same set of rules. However, most of the conclusions and the perspectives offered by this thesis have been drafted by considering the implications of food consumption by humans. Applying the conclusions of this thesis to feedstuffs will be left to the discretion of future researchers

the recognition of its functionality in ensuring an healthy life for individuals. Considering the difficulties in identifying an individual right to (safe) food in the EU legislation[2], it might be the case that other explicitly recognised rights can contextualise food security and food safety within their remit and serve as a sound basis for further discussion. EU Regulation 178/2002 (General Food Law Regulation, GFLR)[3] is the cornerstone of food and feed law. It provides the general framework for the implementation of national and European food and feed legislation (Johnson and Lichtveld, 2017, para 10.4.1). Recital 1 of the GFLR states that "the free movement of safe and wholesome food is an essential aspect of the internal market and contributes significantly to the health and well-being of citizens, and to their social and economic interests".

Despite recognising the importance of the "safe food - better health" relation, Recital 1 forces us to discuss the presence of an "inconvenient companion", i.e. the freedom to conduct a food business and, in general, the economic implications of food safety legislation. This entails that all the regulatory issues pertaining to the safety of foodstuffs have to be framed by keeping into account the twofold rationale of its most relevant piece of legislation: on the one hand, it is intended to promote individual well-being, consistently with the general commitment of Western countries derived

[2] In the EU context, the European Charter of Fundamental Rights (EUCFR) does not explicitly recognise the existence of a "right to food", nor a "right to have a safe food". Despite its absence, scholars have argued that the right to food has been indirectly recognised by the EU, following two approaches. On the one hand, the Union is actively engaged in several international cooperation programs related to food security. European Parliament resolution of 27 September 2011 on an EU policy framework to assist developing countries in addressing food security challenges clarifies the scope of these programs. It has been put into practice through Regulation 233/2014 that establishes Development Cooperation Instruments involving third countries. Food security is mentioned as a key area of cooperation (Annex II.c). A different argument brings forth human rights obligations from international treaties in which the EU is party (Ahmed and de Jesús Butler, 2006) and poses as an example the ACP-EU Partnership Cotonou Agreement. By means of this treaty, the International Covenant on Economic, Social and Cultural Rights (ICESCR) has a direct application on the EU via the reference to economic, social and cultural rights - thus, including the right to food contained in the ICESCR - in Article 9 of the Cotonou Agreement (Gruni, 2018). On the other hand, the existence of a right to food has been justified by the supreme value of human dignity recognised by the Article 2 of the Treaty on the European Union (TEU) and Article 1 of the EUCFR. Advocates of this approach suggest that "all human beings have a right to live in dignity, free from hunger" (Ziegler et al., 2011, p.15) and ground their hypotheses on the General Comment 12 of the Committee on Economic, Social and Cultural Rights of the UN Economic and Social Council on the right to adequate food. The Committee stated that "the right to adequate food is indivisibly linked to the inherent dignity of the human person"(United Nations Committee Economic, Social and Cultural Rights, 1999). Such dignity-based perspective justifies the goal of ensuring freedom from hunger and malnutrition by considering them as pre-conditions for the maintenance and development of physical and mental faculties (FAO, 1975). Human dignity may serve as a justification for tools promoting food security (Ayala and Meier, 2017). However, the concept of dignity is unclear and prone to multiple interpretations across jurisdictions (McCrudden, 2008). Such differences imply that doubts on a dignity-based justification of the right to food still persist.

[3] Regulation (EC) No 178/2002 [2002] OJ L 31/1

from international law; on the other hand, it aims to foster the free movement of foods and the flourishing of the internal market, made necessary by the lengthening of the food chain and the necessity of erasing trade barriers (Szajkowska, 2012, p.21). Therefore, at least two fundamental rights granted by the European Charter of Fundamental Rights (EUCFR) come then into play: the right to physical integrity (Article 3 EUCFR) and the freedom to conduct a business (Article 16 EUCFR). Hence, positive obligations in eliminating barriers to trade and circulation of goods (Article 28 TFEU) and guaranteeing a high level of health protection (Article 35 EUCFR, Article 168 TFEU) can be found.

Health protection is also a limit to the free circulation of goods[4], since restrictions for reasons connected to the health of humans, animals and plants may apply (Article 34 TFEU). Hence, assessing the level of safety of foods (and feeds) is extremely important both for consumers and for the industry and efforts have to be made to ensure that only safe food is placed on the market and its level of safety is correctly assessed. To do so, the European Food Safety Authority (EFSA) is the EU institution responsible for the scientific evaluation of food safety risks. Its mandate derives from the GFLR and it is placed within the context of risk analysis[5], together with risk management and risk communication. The EU Commission and the EU Parliament are responsible for risk management, i.e. taking decisions concerning authorisations, bans, and food recalls, settling legislation, goal-setting, etc. Their decisions are informed by EFSA, which performs the scientific assessment of threats to human or animal health and the environment[6]. Risk assessors and risk managers are jointly responsible for risk communication, i.e. raising risk awareness among consumers, deploying food recalls messages, and so on.

[4] In general, this balance has been found by the CJEU in its *Cassis de Dijon* landmark case, *Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein* [1979] ECLI:EU:C:1979:42, and has been applied consistently in the subsequent case law

[5] For a complete list of EFSA competences - also discussed in Chapter 3 - please see (Alemanno and Gabbi, 2016, p.24)

[6] Art. 114(3) of the TFEU states that "The Commission, in its proposals envisaged in paragraph 1 concerning health, safety, environmental protection and consumer protection, will take as a base a high level of protection, taking account in particular of any new development based on scientific facts. Sectoral legislation often requires the Commission to provide information on the reason underlying outputs that diverge from scientific findings (Alemanno and Gabbi, 2016, p.40) (Krapohl, 2004)

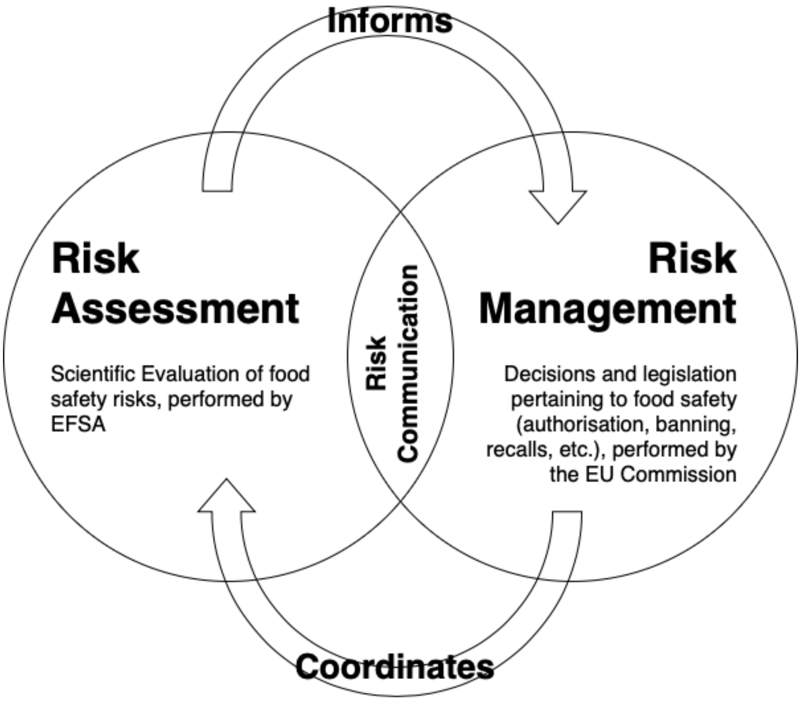

Informs
Risk Assessment
Scientific Evaluation of food safety risks, performed by EFSA
Risk Communication
Risk Management
Decisions and legislation pertaining to food safety (authorisation, banning, recalls, etc.), performed by the EU Commission
Coordinates

Figure 1.1: Risk assessment, risk management, risk communication

As explained by EFSA itself, the growing use of Information & Communication Technologies (ICTs) to analyse products and chemicals used in the food industry has increased the importance of data in risk assessment activities (Cappè et al., 2019). The third external evaluation of EFSA has highly recommended to "keep the pace" with Big Data developments, while recognising EFSA's "ambitious plans for data"[7]. In the near future, this relevance is going to extend still further in light of two main factors to which great attention will be devoted in this dissertation. On the one hand, the collection and storage of data is now a consolidated trend among Western food safety authorities, in particular EFSA. On the other hand, advanced data analysis techniques are increasingly used in this domain. Interestingly, EFSA has no laboratories and cannot perform independent studies, unless scientific uncertainty persists after its evaluation and according to the procedures described in Chapter 3 of this thesis. Hence, most of the data at its disposal are made available either by the industry submitting information pursuing an application or by independent researchers that divulge their findings and correlated data, including on the basis of procurements (EFSA, 2015b; Simpson, 2016). Differently from experimental data, scientific literature is an important source of textual information directly available

[7] The Third Independent External Evaluation of EFSA 2011 - 2016, p. 32 (available at: https://www.efsa.europa.eu/sites/default/files/3rd-Evaluation-of-EFSA_Final-Report100818.pdf)

for analysis.

Preliminarily, the ongoing de-materialisation of food safety risk assessment has to be noted. While the safety of foodstuffs has always been a pressing concern for mankind, the methods to assess if something is safely edible have changed over time. In the last 150 years, due to the progressive industrialisation of society and the consequent enlargement of the food chain, sources of contamination and poisoning have spread across different agents and jurisdictions. Luckily, the contextual development of food microbiology and advances in medicine, as well as legislative interventions to regulate food safety, have had a positive impact on the efficacy of risk assessment practices (Griffith, 2006).

Originally, tasting *all* the foods right before consumption was the only form of risk assessment in Ancient Rome. "Food tasters" were often appointed by rule-makers - nobles, kings and emperors - to prevent food poisoning, an easy way widely used to kill opponents[8].

Then, microbiology relied on the observation of samples to detect harms and investigate potential solutions. The "golden age of food microbiology" (Griffith, 2006) started in 1888, when Gärtner associated 57 cases of Gastroenteritis in Frankenhausen (Saxony, Germany) to a *Salmonella enteritidis* bacterium (Nomenclature Committee of the International Society for Microbiology et al., 1934), and continues to date. As stated above, thanks to microbiology and food safety law, developed countries have become safe places to eat.

In the future, the increasing use of data to classify risks and generate predictions will further de-materialise food safety risk assessment. Throughout this thesis, trend will be referred to as an ongoing "datafication"(Mayer-Schönberger and Cukier, 2013) process, whose peculiarities and implications will be progressively identified. It can be preliminarily observed that this trend has two main facets: *ontologically* speaking, the concept of food and associated entities (consumption, genetic modifications, placement on the market, and so on) is translated into computable objects through three kinds of informational components to which attention will be devoted (human, natural, machine-generated); in the *epistemic* perspective, the computability of food and the same components entails that ICTs can be used to understand the implications of food-related behaviours and draw machine-supported or machine-generated inferences.

This transformation does not imply that a completely "synthetic" form of risk as-

[8] However, the employment of food tasters did not prevent occasional murders. For instance, Emperor Claudius was killed by his own food taster, Halotus, who poisoned a portion of mushrooms eaten by Claudius. It is likely that Halotus was involved in a conspiracy lead by Agrippina to bring Nero to the throne, but there was not enough evidence to convict him (Grimm-Samuel, 1991)

sessment that is detached from real and tangible food and samples would be possible. Even in the most futuristic and "datafied" scenario, foodstuffs will likely remain necessary components of safety risk assessments since they are the ontological and epistemic centre of the analysis[9]. Nevertheless, the presence of artificial agents that cooperate with scientists to predict trends in outbreaks or to identify contingent risks is likely, seemingly to what happens in the biomedical context (Morley, Machado, et al., 2020). The "great promise", aligned with UN SDGs and remote risk assessment, is that everyone on Earth will benefit from such advances.

Today, even though the datafication of risk assessment is tangible and algorithmical evaluation methods are rapidly developing, microbiology and traditional methodologies are still relevant. As we live in the "mangrove society" (Floridi, 2018), technological advances are shaping a domain in which the relevance of data is becoming equal - if not higher - to the one of the observation of real and tangible food. In the course of its de-materialisation, datafied and data-centric food safety generates opportunities and risks.

Several reasons can be attributed to the rise of computational approaches to risk assessment. Similarly to other domains, they might certainly include the availability of larger quantities of structured and updated information - usually referred to as "Big Data" - and sufficient computational power to analyse them in novel forms, including machine learning (Floridi, 2014, Ch.3). This trend is not specific to food safety, but this domain is perhaps one of the least discussed. While commentators have already noted that digital technologies have the potential to enhance the interoperability of data, hyper-linking knowledge, performing aggregate analysis and visualisation also in food safety (Alemanno, 2014, p.213)(Marvin, Janssen, et al., 2017), a detailed study of these phenomena in this domain and their social and legal implications is still missing.

[9] Risk assessment shall also be conceived as an epistemic activity and, as such, it implies some degree of *understanding* in the sense given by Durante (Durante, 2019, p.192). As he argues, understanding is an exclusive capacity of humans even though we are progressively adapting the environment to make it suitable to artificial agents (Floridi, 2014, ch.2)(Durante, 2019, p.236) to which we delegate some epistemic-related tasks. However, the activity of *understanding* cannot be delegated to non-human agents

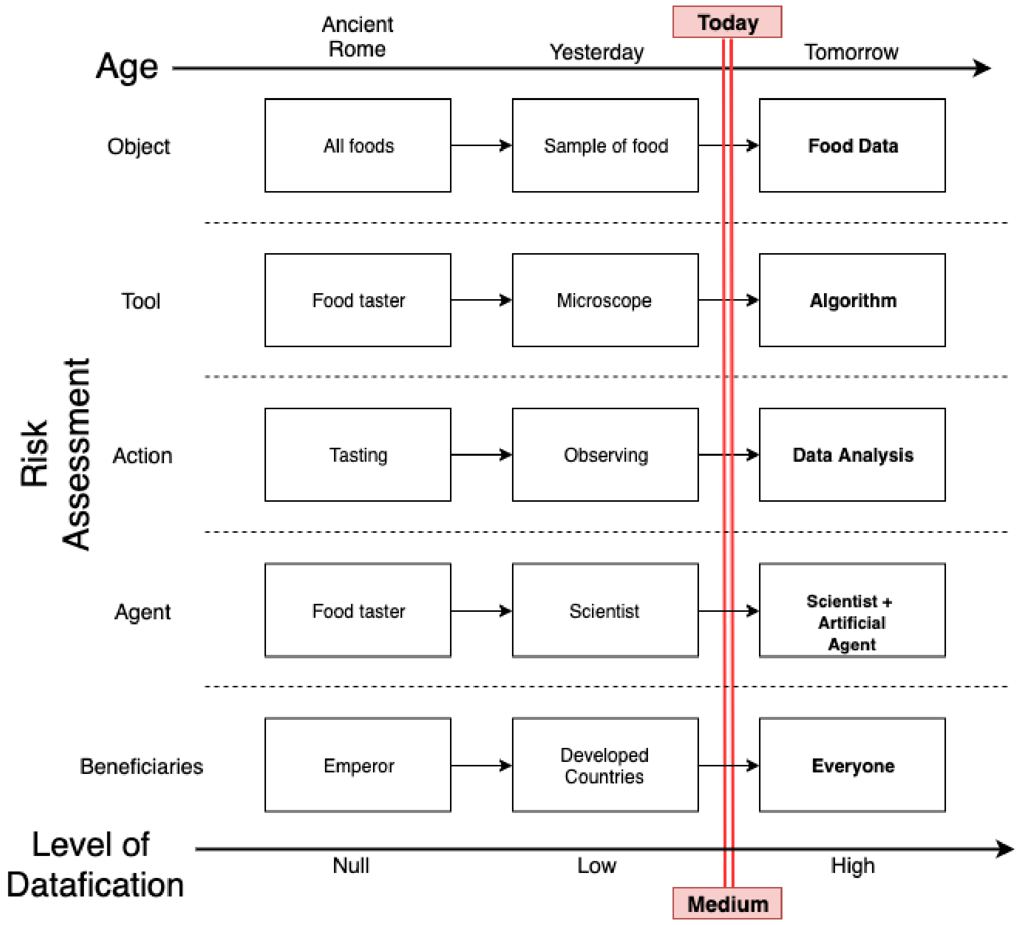


Figure 1.2: Past, Present and Future of Food Safety Risk Assessment

Intuitively, it can be argued that risk assessment is concerned with knowing the consequences of the occurrence (or absence) of certain factors in a given food-related context. For instance, the use (occurrence) of pesticides (factor) in agriculture (context) is a typical and highly controversial setting in which risk assessment is performed to evaluate whether or not pesticides could be considered "safe". In principle, we could have knowledge about the safety of factors by observing the presence of the factor itself for a sufficient amount of time in the context at stake and evaluating its effects. Such timespan can range from few hours to years or decades.

Food Safety and data analysis

The following example shows how data analysis can enhance food safety risk assessment with regards to a parasite[a].

Harmful effects on humans of parasite (factor) such as *Opisthorchis viverrini* (it might be infective to humans through ingestion of raw or undercooked fish (context)) - which include cholangiocarcinoma - could be observed only after 30-40 years (Sripa et al., 2011). This has been the case for Vietnam veterans, whose consumption of food is an infected area has been linked to the cancer only in 2018 (Psevdos et al., 2018). This timespan is naturally needed by the parasite to develop, move to intermediate host, then to the final host, and generate harm; however, the detection of this contaminant in food is a matter of days (FDA, 2017). Large, structured and updated data can significantly improve both the identification and the evaluation of risks connected to parasites. To identify *Opisthorchis viverrini* and other pathogenic helminth eggs, Jimenez and colleagues used 720, 2560-1920 pixel, images to train a naïve bayesian classifier software capable of detecting the presence of parasites' eggs in wastewater (Jiménez et al., 2016). Its sensitivity and specificity were respectively 99% and 80-90%. These promising results could foster the deployment of precise and less costly systems, which could also operate by remote distance (e.g. in developing countries or in rural areas). At the same time, three different computational algorithms (maximum parsimony, maximum likelihood, and Bayesian analysis) were used in another study to perform phylogenetic analysis of the same parasite [b] (Cai et al., 2012).

In the example reported above, data analysis may clarify both the presence of a contingent risk (the parasite) and the likelihood of its long-term effects (clonorchiasis). On the one hand, the detection of tangible harms can be associated to a classification problem (presence vs. no-presence); on the other hand, forecasting the consequences of harmful entities - including chemical substances contained in pesticides - can be described in terms of developing a prediction model.

[a] Other examples - including the more controversial scenarios regarding pesticides - will be discussed in Chapter 2

[b] Phylogenetic analysis aims to find common evolutionary relationships among organisms (*taxa*), usually represented in form of dendogram.

Food safety risk assessment mostly concerns reducing the uncertainty and increasing the predictability of possible hazards. While the aforementioned opportunities in predicting and detecting risks illustrate the potential of data analysis in food safety risk assessment, some risks may emerge from its deployment in this domain. Before introducing them, it may be relevant to identify two intertwined factors that contribute to originate some controversies with the regard of the datafication of risk assessment.

On the one hand, the food business operators submitting data to the risk assessor (EFSA) are not keen on releasing data into the public domain. A strong commercial interest in the protection of the investments needed to gather and analyse data can be easily justified for the research and development (R&D) costs incurred by the industry to place their new products on the market[10].

However, such position clashes with the public interest in accessing these data in order to perform independent reviews and analyses, in particular regarding areas of scientific uncertainty like plant protection products (PPP) or Genetically Modified Organisms (GMOs) or where environmental information is concerned. This position is safeguarded by international conventions and EU law at several level, as it will be discussed more in detail in Chapter 3. The presence of such conflicting interests hinders the finding of shared solutions - including data governance measures - intended to maximise the benefits of data analysis. Among other areas, public availability of data and competition within the industry are two of the most affected sectors.

On the other hand, modern data analysis practices pose new and unknown risks related to the nature of the processing. For instance, algorithmic transparency - intended as explainability, explicability and "scrutinisability" by EFSA - is a prime concern due to the well-studied difficulties in understanding the logic underlying certain machine learning approaches (Pasquale, 2015). Furthermore, the protection of commercial interests can put an additional layer of obscurity of the algorithms. Eventually, the combination of "mixed data" - i.e. the contextual analysis of variables representing non-personal and personal data - is very common in this domain. The presence of this factor calls for a discussion on the way in which this combination might be exploited for purposes other than food safety risk assessment or might privilege/disadvantage certain individuals.

Taken together, these intertwined elements[11] contribute to the emergence of risks linked to the lack of trust both in EFSA and in the food industry, the loss of human scrutiny over risk assessment activity performed by algorithms and, eventually, unfair or unequal results. As Chapter 3 will discuss more in detail, the legal attempt to redefine the legislative framework in which the food safety risk assessment operates (i.e. the 2019 Transparency Regulation)has left some of these issues unresolved.

Years before this amendment,, EFSA has made an attempt to define principles to govern the management of data and evidence (EFSA, 2015b). The Authority have stated that data analysis in risk assessment has to be carried out according to principles of impartiality, excellence in scientific assessments, transparency and open-

[10] A detailed analysis of the costs will be provided with regards to Genetically Modified Foods and Feeds at §3.1.2

[11] The two factors presented above have to be intended as correlated rather than isolated. The reason underlying their separate description is their focus. While the first is mostly concerned with the accumulation of large quantities of structured data by the industry, the second is mainly referred to the way such data is analysed. More on this topic will be discussed in the next section

ness, and responsiveness. While these principles have to be taken into account for their significance as relevant guidelines for all the concerned stakeholders, their resilience to innovations discussed in Chapter 2 has yet to be verified.

If the adopted reform and EFSA's attempts are partly insufficient or not sufficiently forward-thinking, the need of ethical contributions is necessary to integrate, interpret and align this piece of legislation to the principles enshrined in policy documents emerged from regulators, experts, technicians, and scholars active in the field of data ethics. To contribute to this far-reaching goal, this dissertation aims to draft an "Ethical Roadmap" for a responsible and trustworthy innovation in the fields of data-based food safety risk assessment. However, it is first necessary to find an appropriate workflow by preliminarily defining the most relevant concepts under discussion, the research questions and an operative methodology. The following sections describe these crucial points.

1.2 Key definitions

The sections below aim to briefly define some necessary cornerstone concepts that will be used throughout this thesis. This is mainly intended to illustrate some consolidated definitions in the literature, underline the semantic ambiguity of certain terms and conveniently define concepts in a manner that fits our purposes. By deconstructing and reconstructing some possible interpretations, highly - yet, unavoidable - arbitrariness in defining terms should be prevented on account of an objective scrutiny. Finally, the proposed interpretations have to be intended as working definitions strictly confined to the purposes of this dissertation. Therefore, there is no claim to the universality of these conceptualisations.

1.2.1 Food Safety Risk Assessment

Food safety risk assessment will be described under two perspective, a *substantive* and a *procedural* one. In general, the notion of risk assessment encompasses: a) food use (e.g. consumption, preparation, cooking, etc.), intended or effective, including those of certain categories (e.g. children); b) immediate, short-term, long-term effects of the usage; c) cumulative negative effects of the use (Rusconi, 2016, p.462).

From a *substantive* point of view, risk assessment consists of four steps (Gilsenan, 2015):

1. **Hazard identification** aims to identify negative health effects (e.g. carcino-

genicity) that may be caused by the exposure to a particular agent, regardless of the known/unknown nature of the agent itself. This step mainly consists of the review of the scientific literature on hazards.

2. **Hazard characterisation** measures the relationship between a certain level of exposure and the occurrence of negative health effects.

3. **Risk characterisation** measures the concrete level of exposure by identifying the level of hazard in food eaten in a given area/time/population.

4. **Exposure assessment** relies on hazard characterisation and exposure assessment data to predict how likely a certain risk scenario will materialise.

From a *procedural* perspective, the risk assessment protocol[12] is based on the following steps:

1. **Request**. EFSA can be tasked for scientific advice by the EU Parliament, national food safety authorities or the EU Commission (including on the basis of a request coming from the industry, i.e. to place a regulated product on the market if the requested use might have an effect on human health[13]). EFSA can also act on its own initiative in the field of emerging risks.

2. **Mandate**. If accepted, requests become mandates.

3. **Assignment**. Mandates are assigned to Panels of scientific experts (thematic working groups) or the Scientific Committee (a board in charge of harmonising findings and methodologies). Scientific panels include:

   (a) Pesticides

   (b) Animal feed

   (c) Animal wealth and welfare

   (d) Biological hazards

   (e) Contaminants

[12] The procedural perspective described hereafter is derived from the general procedure followed in the EU

[13] Commission Regulation (EU) No 234/2011 of 10 March 2011 implementing Regulation (EC) No 1331/2008 of the European Parliament and of the Council establishing a common authorisation procedure for food additives, food enzymes and food flavourings [2011] OJ L 64/15

   (f) Nutrition

   (g) Food additives

   (h) Food contact materials

   (i) Genetically Modified Organisms

   (j) Plant Health

4. **Working Group.** The Panel or the Committee select experts set up a working group. It performs the risk assessment by relying on the expertise of its members, scientific data and scientific literature.

5. **Draft Opinion.** The Working Group publishes a draft opinion by making it available to the Panel or the Committee and occasionally to other experts and stakeholders, which contribute with additional data, literature and feedback.

6. **Review and Adoption** The Scientific Committee or Panel reviews the feedback received and drafts the final opinion, which is adopted by consensus.

7. **Divulgation.** Once adopted, the Opinion is sent to the requester and published on EFSA Journal, freely accessible on the Internet under open access conditions and Creative Commons Attribution License (CC-BY-ND) licence.

1.2.2 Big Data

‘Big Data’ is an ambiguous term. Mittlestadt and Floridi (Mittelstadt and Floridi, 2016) affirm that there is no unique understanding of the concept Big Data in philosophical terms, nor it has been found by an extensive review of the technical literature on the topic (De Mauro et al., 2015). Hence, an arrogant claim to a universal definition of Big Data cannot be made here. Instead, this section will attempt to set a working definition for the purposes of this dissertation and explain why a certain conceptualisation should be preferred among other alternatives.

Attempts made to define Big Data can be broadly divided into three categories: the *quantitative*, the *qualitative*, and the *reductionist* approach. As their names suggest, these perspectives provide a different angle to tackle the definitory issue. They emphasise the adjective "big" by differentiating its meaning either by highlighting the size of the entity to which "big" refers to ("big" as in "a big tree"), by focusing on some qualitatively relevant peculiarities ("big" as in "a big deal") or by answering to the question "*what* is big?" in Big Data.

In contextualising Big Data, all the aforementioned approaches have implicitly relied on the notion of "information" deriving from information theory, which does not take into account the semantics of data[14].

The *quantitative* approach highlights the dimensional meaning of the adjective "Big" by identifying Big Data as all those datasets whose dimension reaches or exceeds a given quantity. For instance, the exabyte (10^{18} bytes) has been used to delimit the threshold that separates "regular" data from "big" data (Kaisler et al., 2013). Similarly, sounding expressions like "Zettabyte Era" (10^{21} bytes) have been used to describe the "massive amounts of data" collected and analysed in our age (McNeely and Hahm, 2014). Broadly speaking, we face a quantitative approach to Big Data when emphasis is placed on the accumulation of digitalised information.

The *qualitative* approach primarily focuses on the complexity of the data set and the number of *ad hoc* measures that have to be adopted for its management. Following this approach, it has been affirmed that "Big Data is data that exceeds the processing capacity of conventional database systems" (Dumbill, 2013). MIKE (Method for an Integrated Knowledge Environment) 2.0 has stated that "Big Data that is very small" and that "large datasets that aren't big" may exist. As an example, it is reported that even though the 100,000 sensors of a commercial aircraft may originate a relatively small amount of data (3GB/h), the diversity of data sources requires special measures for the handling of this information. Conversely, well-organised relational datasets can reach massive dimensions without needing additional measures for storage or computation such as distribution or parallelisation.

The *reductionist* approach breaks the concept of Big Data into smaller components to ease its understanding and identify its essential traits. Several authors have followed a narrative based on "V"s. First, Douglas Laney proposed a tripartition of Big Data into *Volume*, *Velocity* and *Variety* (Laney, 2001): Volume identifies the dimensional aspect of Big Data; Velocity is related to the update frequency of this information; Variety describes the presence of heterogeneous formats (e.g. photos, web pages, personal information, audiovisual) that can combined in a single operative framework and the need of "linking" formats, such as XML. Taking inspiration from Laney's work, others expanded his definition by adding further "V"s. IBM (IBM, 2014) included "*Veracity*", i.e. the necessity of having high quality data to prevent false results. Moreover, the American company added a further "V" by identifying "*Value*" as the economical component of Big Data (IBM, 2016). A neighbour definition is also part of ISO/IEC 20546 (para. 3.1.2) concept of Big Data, which also takes into account the technology used to manage extensive databases.

[14] Shannon's information theory (Shannon, 1948), taken by itself, adopts a strictly technical approach. In his own words: "[F]requently the messages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem".

Several drawbacks affect the first two approaches. The concept of quantitative "dimension" shall not be intended in a physical sense. Authors who adopted a quantitative approach had in mind the immaterial size of data, usually measured by units such as "kilobytes" or "terabytes". However, the threshold that separates "regular" data from "big" data is highly discretionary[15]. Similarly, authors who adopted a qualitative approach would need to adapt their definition to the state-of-the-art in database management, equally falling in arbitrariness as the others[16].

Despite avoiding this pitfall and being far more stable, the narrative proposed by the reductionist approach brings with it the issues of methodological reductionism, i.e. the impossibility of defining (rather than describing) something by integrating high-level features in a holistic manner. However, the peculiarities described by this approach fruitfully combine the two meanings of "Big" explained at the beginning of this subsection, thus being a reliable starting point for our working definition.

The gaps left open by the "V"s narrative in defining "data" could be filled by using other contributions, for instance the ones that describe its philosophical concept.

From a philosophical point of view, the reconstruction operated by Floridi (Floridi, 2013b) has been described as an attempt to identify a "philosophically technical concept of semantic information" (Lombardi et al., 2016) that allows us to discuss the larger picture of Big Data other than signals transmitted through a channel. Floridi argues that a *Datum* is an ontological "lack of uniformity" (Floridi, 2013b, p.85)[17] in the world.

The concept of data includes: *primary* data (i.e. array of numbers stored in a given support), *secondary* data (i.e. the absence of data, like the silence in a communication), *metadata* (i.e. indications related to primary or secondary data), *operational* data (i.e. data about the functioning of an information system) and *deriva-*

[15] It is worth noting that the cited authors have adopted different thresholds, thus making their arbitrary choices unreliable from a definitory point of view. Moreover, frequent adaptations would be needed to adapt the threshold to the well-known growing amount of data generated in our age and discussed in their papers.

[16] In principle, nothing would prevent us from adoption either one of the perspectives. If that were the case, we would simply need to adapt the amount of data that identify Big Data (in the quantitative scenario) and investigate the average processing capability of a given sector (following the quantitative approach). However, relying on either of the approaches would make our definition depending entirely on external factors subject to change, thus compromising the validity of our findings in the long period

[17] Floridi discusses following diaphoric interpretation, based on differences. Divergences can be observed in the real world (Data as diaphora *de re*), in the perceptions of signals, e.g. Morse code lines and dots (Data as diaphora *de signo*) and among symbols, for examples two letters from an alphabet (Data as diaphora *de dicto*). It follows that different symbols encode different signals that reveals anomalies around us

tive data (i.e. data that can be generated from some other data where the latter is used as the source of patterns and inferences). The relationship between "data" and "information" is then completed by keeping into account the Level of Abstraction (LoA) through which an epistemic agent encapsulates data into information (Durante, 2017, p.86)[18]. While the latter should not necessarily be included in a data-centric definition of Big Data, keeping into account agents and LoAs is necessary to describe and analyse the processes that transform data into information[19]. If the agent and LoAs have to be considered, our definition could also include technical and legal classes capable of describing how the agent understands data as engineering problems and how legal norms classify data before generating rights, obligations, sanctions, and so on.

From a technical side, the description of "data" is seemingly compatible with the philosophical one. ISO/IEC 20546 (para. 3.1.5) specifies that data is a formalised representation of information. A taxonomy provided by the Information Accountability Foundation (Abrams, 2014) and publicly endorsed by the UK Information Commissioner's Office (ICO, 2017) outlined that data can also be described by looking at the their origin: *provided* (i.e. originated by a conscious individual), *observed* (i.e. simply recorded), *derived* (i.e. extracted from other data in a mechanical way) and *inferred* (i.e. extracted from other data following a probability-based analysis).

From a legal perspective, the concept of data is mainly based on the identifiability of an individual to whom the data refer to. Following the macro-categories of *personal* data (i.e. any information relating to an identified or identifiable natural person[20]) and *non-personal* data (i.e. every data that is not personal, including anonymous data[21]), in-between classes consist of "*anonymised* data" (i.e. personal data sub-

[18] More on the method of Level of Abstraction will be said in §1.4.3

[19] The inclusion of "derivative data" within our description may generate some confusion. This concept includes inferences and patterns, but it is still represented in an embodied form (e.g. the precision and the recall of a predictive model). Information, instead, is the conclusion that an epistemic agent reaches in lights of data and LoA (e.g. a foodborne outbreak is likely to occur given certain premises)

[20] Article 4 of the Regulation 2016/679 of the European Parliament and of the European 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 [2016] OJ L 119 (General Data Protection Regulation, GDPR) states that personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. For a detailed commentary on the GDPR see the exhaustive discussion by Kuner et al. (Kuner, Bygrave, et al., 2020)

[21] The 2019 EU Commission Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union states that "non-personal data can be categorised by origin as:

ject to an anonymisation processing[22]), "*pseudonymised* data" (i.e. data undergone through a processing activity in such a way that it is not possible to attribute them to a specific person without the use of additional information[23]) and "*mixed* data" (i.e. the combination of personal and non-personal data within the same dataset[24]).

We can finally identify our working definition for Big Data. Noteworthily, the approach taken to find our working definition is purposively holistic. To summarise our attempt to define Big Data, we have relied on the "V"-narrative of their characteristics - volume, velocity, variety, veracity, value - and on the philosophical, technical and legal concepts of "data" to fill the gap of the "V"-narrative. Technical and legal definitions have been included since the philosophical approach also keeps into account an epistemic agent and its behaviour.

1*st* working definition: Big Data

All data - in all their philosophical, technical and legal manifestations - that are characterised by volume, velocity, variety, veracity and value.

1.2.3 Machine Learning

In its simplest definition, Machine Learning is a capability of computers "to adapt to new circumstances and to detect and extrapolate patterns"(S. Russell and Norvig,

Firstly; data which originally did not relate to an identified or identifiable natural person, such as data on weather conditions generated by sensors installed on wind turbines or data on maintenance needs for industrial machines. Secondly; data which were initially personal data, but were later made anonymous. The ‘anonymisation’ of personal data is different to pseudonymisation, as properly anonymised data cannot be attributed to a specific person, not even by use of additional data and are therefore non-personal data."

[22] More specifically, the Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques sets a three-step test to identify the robustness of anonymisation techniques. It should not be possible: to identify an individual, link records relating to an individual and to infer an information concerning an individual

[23] Regarding pseudonymised data, the Commission clarified that "data which have been pseudonymised are still considered information about an identifiable person if they can be attributed to this person by using additional information. Such data constitute personal data in accordance with the General Data Protection Regulation". This implies that a case-by-case analysis would be necessary to assess whether or not stored data are personal or not. However, considering that "’anonymisation of personal data is different to pseudonymisation", pseudonymised data should be conceived as a stand-alone concept

[24] The 2019 EU Commission Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union states that "a mixed dataset consists of both personal and non-personal data. Mixed datasets [...] are common because of technological developments such as the Internet of Things (i.e. digitally connecting objects), artificial intelligence and technologies enabling big data analytics"

2010, p. 2). Machine Learning aims to find an acceptable, statistical and probabilistic generalisation - to which this thesis will refer to as a "statistical model" - calculated from input data. In other word, a Machine Learning algorithms aim to extract a pattern from the known values of a *predictor* variables to determine the value of a *target* variable. This entails that a) results are always expressed in terms of a probability and b) the statistical model expresses statistical correlation rather than causation (Kantardzic, 2011).

This capability is strictly related to the availability of Big Data. As Russel and Norwig explain when discussing post-2000 trends of Artificial Intelligence[25] (AI), "[t]hroughout the 60-year history of computer science, the emphasis has been on the algorithm as the main subject of study. But some recent work in AI suggests that for many problems, it makes more sense to worry about the data and be less picky about what algorithm to apply. This is true because of the increasing availability of very large data sources" (S. Russell and Norvig, 2010, p. 28).

Within the broader category of AI, Machine Learning is subset (European Commission, 2020) consisting of a statistical approach placed between symbolic and subsymbolic paradigms (Corea, 2019), two branches that reflect the difference between the Symbolists and the Connectionist approaches (S. Russell and Norvig, 2010, p. 24).

[25] Given the abundance of literature on this topic, this dissertation will not discuss in detail the definition of Artificial Intelligence. Originally, it was conceived as the "making a machine behave in ways that would be called intelligent if a human were so behaving" (McCarthy et al., 2006, as previously stated in AI Magazine, 27(4), 12 (1955)). Traditionally, AI can be defined according to four approaches, i.e. the ability of a machine either to reproduce human thinking or human acting, or to think or behave rationally (S. Russell and Norvig, 2010, p.2). Research interests also include future trends and superintelligence (Müller and Bostrom, 2016), the role of AI in philosophy of mind (Clark and Chalmers, 1998), and morally-relevant artificial agents (Floridi and Sanders, 2004)

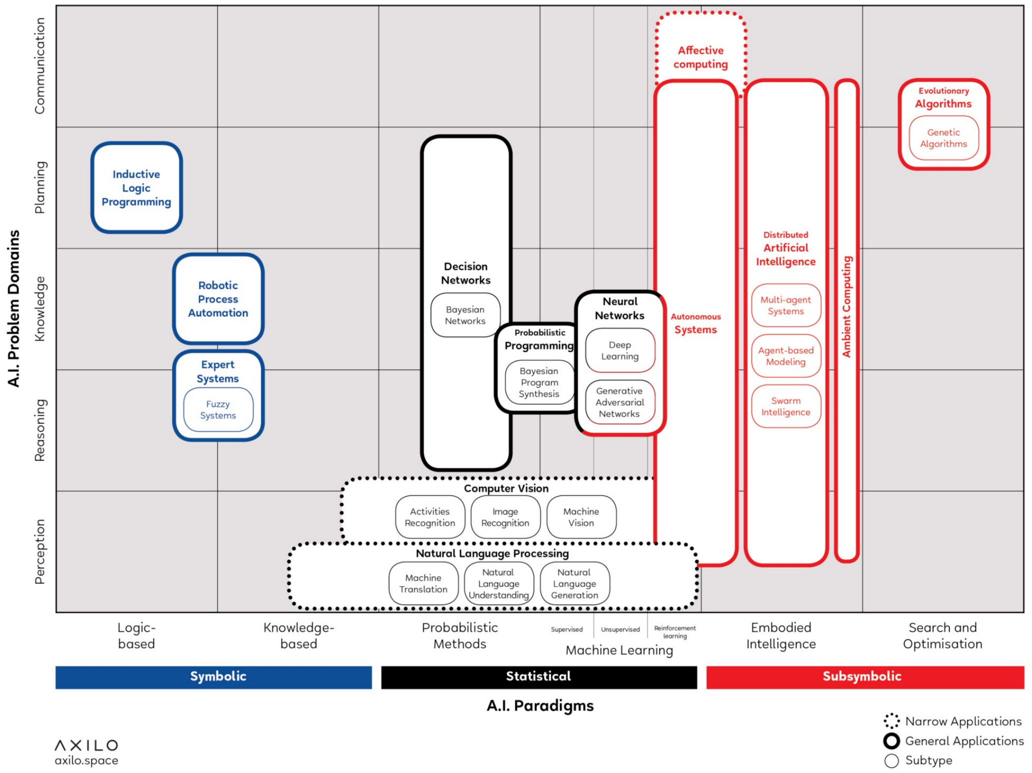


Figure 1.3: AI Knowledge Map (AIKM) (Corea, 2019)

Symbolic approaches to AI attempt to process input symbols according to predefined explicit rules which mimic human's mind activity in order to produce an output. Symbolic tools may consist of logic-based (i.e. based on logically-constructed rules) or knowledge-based (i.e. based on ontologies) rules. This entails a low flexibility in dealing with new and unprecedented scenarios, i.e. those unknown to the algorithm. Let us consider the case of face recognition. The programmer provides the system with a pattern to recognise. The system is instructed with explicit rules, which have to be sufficiently precise when describing the components of human faces (e.g. two eyes (oval-shaped), one nose (curved), one mouth, hair, made of a certain amount of pixels of a given colour). When the algorithm finds these components in the input image, it returns a "`is_face = TRUE`" statement. Vice versa, the output of the classification would be "`is_face = FALSE`"

Subsymbolic approaches provide no *a priori* knowledge to follow for computer reasoning. Evolutionary algorithms, for instance, let the algorithm "evolve" through a sequence of steps that mimic human evolution, including generations, mutations and the survival of the best candidate in any generation. As it will be discussed, this comes at the cost of explaining the reasoning of the algorithm and its results

(Pasquale, 2015). Considering the previous example, subsymbolic approaches have been successfully used to search and normalise components of human faces (Wong et al., 2001) in the following ways.

These statistical paradigms aim to solve complex problems by means of mathematical rules without an *a priori* knowledge base. While probabilistic methods rely on Bayesian statistics and incomplete information, Machine Learning extracts these rules directly from data. Following our example, in Machine Learning the programmer first provides the algorithm positives ("faces") and negatives ("non-faces"), then lets the algorithm extracts the pattern recognition rules (i.e. eyes, nose, etc.)

Machine learning is commonly used to solve two kinds of tasks:

- **Classification problems**, in which the number of possible values for the target variable is finite (e.g. "faces" vs "no-faces")

- **Regression problems**, in which the number of possible values for the target variable is infinite (e.g. weather forecast)

Machine learning algorithms can be divided into certain categories:

- **Supervised learning** aims to find patterns between labelled variables/predictors to infer the value of a target variable. Hence, the generation of a statistical model requires a training dataset - manually annotated or labelled - like the one in the example above ("faces"/"no-faces");

- **Unsupervised learning** aims to find patterns between data points to organise and represent them without the need of labelled variables;

- **Semi-supervised learning** consists of a hybrid method needed when a limited amount of labelled data is available;

- **Reinforcement learning** makes algorithms choose an action on the basis of the enviroment in which they are deployed. Eventually, they get penalised or rewarded on the basis of their actions

- **Ensemble methods** consist of the combination of two or more approaches.

2nd working definition: Machine Learning

Machine Learning is the subset of Artificial Intelligence that aims to build statistical models from pattern recognition and extraction, to be used for classification or regression tasks.

1.2.4 Data Ownership

This section aims to define a working definition for another core concept of this dissertation: data ownership. With the concept of "data" being defined in §1.2.2, we can focus on how the concept of ownership applies to it. While we will refrain from using other expressions, including "data control" (House Of Lords Select Committee, 2018, para 62), it is necessary to acknowledge that contextualising ownership into data poses unique challenges for the reasons expressed below.

Ownership has been defined by the Oxford Dictionary of Law as "an exclusive right to use, possess, and dispose of property, subject only to the rights of persons having a superior interest and to any restrictions on the owner's rights imposed by agreement with or by act of third parties or by operation of law" (Martin, 2009). Hence, ownership rights are mainly characterised by exclusivity, with the interference of external agents being exceptional. However, in a "data ownership" scenario the concept of "exclusivity" is put under a significant stress by the nature of the commodity at stake[26].

Consistently with this exclusion-based discourse, rules that prevent or allow external agents from accessing data can generate at least four models of ownership. Scholars who attempted to categorise commodities in terms of *exclusion* (i.e. how difficult is excluding a person from enjoying a given good) have also included the concept of *substractability* or *rivalrousness* (i.e. whether the use made by an agent prevents others from using the same good). Following this approach, they can be defined either as public, private, club goods, or as common-pool resources (CPRs) depending on their excludability and rivalrousness (Borgman, 2015).

Table 1.1: Categorisation of goods in terms of excludability and rivalrousness

		Rivalrousness	
		Low	High
Excludability	Difficult	Public Goods	Common-pool Resources (CPRs)
	Easy	Toll or club goods	Private goods

We can observe these models of ownership through our data-centric lens. This

[26] In the previous section, the concept of data-as-a-commodity was not addressed. Our assumption is the following: whenever something that we have defined as "data" is treated on a par with tangible objects rather than a digital formalisation of lack of uniformity in a given environment, these data become commodities or assets. Hence, when data are treated as "goods", legal rules may constitute rights, prescribe obligations, and so on.

approach will not follow two main considerations made by the British Academy (British Academy and Royal Society, 2019). First, the discourse on data ownership should not be confined solely to personal data. This is necessary to avoid inconsistencies with the scope of our investigation, which also includes other types of data. Second, that data are non-rivalrous-*by-default*. It is a fact that data reproduction costs are infinitely lower than their material counterparty[27] and this factor has tricked many into thinking that rivalrousness of data cannot simply exist, as a simple "copy-paste" operation would allow any potential user to access digital information. However, this is not always true, since technological or legal constraints may be put in place to prevent access to data in a way that only a limited number of users at the time can a given piece of information (DECODE project, 2020; Mahmoud, 2019).

Some data are characterised by low subtractibility/rivalrousness and difficult exclusion. This is the case of all the information which is made available to the public without any technological, economic or legal restrictions. For instance, "open data" - broadly defined as those data "in an open format that can be freely used, re-used and shared by anyone for any purpose"[28] or which “anyone can freely access, use, modify, and share for any purpose (subject, at most, to requirements that preserve provenance and openness)" (Global Open Data Index, 2019) - can fall under the category of public goods.

Club goods are characterised by easy excludability but low rivalrousness. In the "material" world, a golf course is a "club good" as it offers a member-only entrance for a large, non-rivalrous space. In our context, datasets that are subject to subscription-based access rules - such as case-law online repositories - or that can be accessed only under certain technical conditions - such as APIs that provide data in a proprietary and non-interoperable format - can be considered club goods.

The definition of CPRs refers to natural or man-made resources that are sufficiently large to make expensive - but not virtually impossible - to prevent others from obtaining benefits from its use (Ostrom et al., 1990, ch.2). A highway is a good example of CPR: it is hard to exclude others from riding it, but it might be subject to congestion. In the immaterial scenario, certain servers allow for a limited amount of possible simultaneous access to the dataset that they keep online[29]. This entails

[27] Let us consider the reproduction cost of a book and its PDF/EPub version. While the costs associated to duplicate the physical book consist of printing, shipping, human resources, time, etc, its digital counterparty only necessitates a few click and, possibly, the electricity necessary to perform the computations linked to the reproduction. Since for most of digital items electricity costs are neglectable (this is not the case, for instance, of blockchain-based technology), reproduction costs of digital items are said to be zero

[28] Recital 16 of the Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56)

[29] It is reported that data kept in a SQL server can be simultaneously accessed by 32.767 users (Microsoft, 2019)

that - despite being (computationally) expensive - individuals could theoretically occupy the hundreds or thousands of spots available to access the data, for instance when a very significant number of devices query the database.

Private data are characterised by easy excludability and high rivalrousness. In this sense, they constitute "private property" of their owner. The legal attribution of exclusive rights over data may derive from intellectual property rights (IPRs)[30]. Similarly, "personal data" are often treated just like "private data" by scholars supporting an ownership-based approach to data privacy (described by Floridi, 2005) and Restricted Access/Limited Control (RALC) theories (Tamò-Larrieux, 2018)[31].

Table 1.2: Categorisation of data in terms of excludability and rivalrousness

		Rivalrousness	
		Low	High
Excludability	Difficult	Open Data	Data with limited access
	Easy	Subscription-based repositories	IPR-protected data

Before proceeding to examine the concept of ownership, it is necessary to explain how certain peculiarities of data might challenge ownership models grounded on exludibility and rivalrousness.

First, the shift from an ownership model to another of the *same exact* encoded digital information is easier than its material counterparty. Let us imagine two copies of a book, namely a book and its *e*-version in PDF/ePub format. While the book - like all the physical items - is normally characterised by high substractibility (usually, only one person at the time can read that copy), the same digital copy can easily be enjoyed by two or more individuals at the same time. Even though ways to prevent such contextual use (e.g. IPRs, licenses, Digital Rights Managements (DRM) tools) can be put in place, these are "artificial constraints" (Rodotà, 2015, p. 132) having regard to the nature of data, which is characterised by very low - and often null

[30] It worth noticing that, in EU law (Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77), IPRs are related to databases. Copyright and *sui generis* protection are respectively intended to preserve the intellectual creation of the database structure and its content if a substantive investment in obtaining, verifying or presenting the database has been made

[31] The Restricted Access/Limited Control (RALC) and ownership-based theories interpret data privacy as the right to limit the amount of information available to other entities are rooted on the psychological desire of secrecy and intimacy (‘right to be let alone’). Following RALC-wise theories, the access to certain "zones" or "spheres" is restricted by the individual to protect himself or herself from external intrusion as personal data were subject to property rights

- reproduction costs as described above. Hence, while transforming the physical book into a CPR by donating it to a library is subject to certain conditions (e.g the approval of a librarian regarding the conditions of the book), the immaterial shift only requires the upload on a private shared folder reachable by the individuals designated by the owner (let us say, his or her friends) according to access limitations set by the service provider[32], with consequences e.g. on copyright[33]. The reversed process is equally feasible: if someone accesses a publicly available copy of an e-book, he or she can easily store it in a private server and make it accessible only through a subscription fee if his or her licence allows so. Instead, finding a way to make private a book that belongs to a public library would amount to theft even when the book has fallen in the public domain.

The impact in terms of the excludability goes hand to hand with subtractability: while the physical book in the public library exists *only once* in its tangible manifetation, thus making excludability hard but not impossible (e.g., if the library that stores that *unique* copy of the book is closed on Sundays), the immaterial copy is accessible 24/7/365 and infinite duplicates can be done to make the book even more available[34], to the extent that the original owner will not have excludability powers over the book, which should conveniently be considered a public good at that point.

However, none of these shifts prevents the original owner from enjoying his or her own digital copy of the book, nor his or her friends to read the copy stored in the shared folder, nor other individuals to access the same copy mirrored on a public website, nor the subscription-based platform to offer the same book to its customers. This property of digital information contributes to the second challenge to classic ownership models: while material commodities might follow one model at a time, the *same exact* immaterial resource can simultaneously follow numerous models (DECODE project, 2020).

To summarise, two major challenges have been raised when trying to adapt the traditional ownership models to a data-centric discourse. On the one hand, the shift of immaterial resources from one model to another is simpler than in their material

[32] For instance, "basic" Dropbox users can achieve a maximum of 20 GB of bandwidth and 100,000 downloads per day (`https://help.dropbox.com/en-uk/files-folders/share/banned-links`)

[33] With regard to this relationship, see also Spredicato (Spedicato, 2016) on the access to digital knowledge and copyright

[34] The description of this process has been purposively simplified. In fact, the authenticity of copied data can always be challenged. For instance, bytes might be lost during the upload/download/copy due to compression algorithms that manipulate the file without compromising the human perception. As a result, while a user could perceive data as a *perfect substitute* when accessing them, some units of information might have changed from the machine's perspective. In our description, we will simply refer to the human understanding of data which is usually not compromised in the course of data transfer

counterparty; on the other hand, the simultaneous presence of multiple ownership models on the same resource can occur more frequently than in the material world. Therefore, a strict adherence to the classic ownership model cannot be pursued. Nonetheless, excludability and subtractability represent a pragmatic description of their hidden premise, i.e. having *control* over certain resources.

In fact, each presented scenario calls for an agent that exercises some degree of power over data: in private data, the agent is the person granted of exclusive rights by the law or by contract; in subscription-based repositories, the agent is the platform that makes the content available to the users; in "open data" scenarios, control depends on the conditions under which data is made available to the public (e.g. Creative Commons licences), but it safe to assume that we are confronted with a decentralised form control democratically exercised through an entity (e.g. public administration); CPRs data can be owned by various entities (e.g. consortia), depending on the way in which the resource is managed (Ostrom et al., 1990, Ch. 3).

The major implication of this paradigm shift is the necessity of conceptualising data ownership as a *scalar* measure. It does not consist of "all or nothing" prerogatives like the traditional and monolithic *ius utendi, fruendi et abutendi* concept of property derived from Roman Law, but it can be conceptualised as a bundle of rights (e.g. access, distribution, etc.) related to informational assets that show some degree of control over the information. A major difference between, let us say, renting a physical book and licensing digital contents is the subtractability of the good at stake: while renting a physical good usually entails the impossibility, for the tenant, to use the object of the renting contract unless the contract is terminated or exceptional circumstances occur, the licensor of data can still use it or make it available to other entities as the copies are perfect substitutes.

The inclusion of data erasure among the faculties attributed to a data owner is somewhat problematic. If *A* attributes some degree of ownership to *B* over data *XYZ*, then it might be the case that *B* can legitimately dispose of *XYZ* to erase them. It has been noted that more than one ownership models can be applied at the same time to the same data. Therefore, it is necessary to differentiate how this erasure can occur: *B* could either destroy his/her copy or erase *A*'s copy. The two cases are relatively common: the former case applies, for instance, when users erase copies of e-books in their e-shelves; the latter usually occurs under licensing conditions, e.g. when digital platforms prevent access to e-books copies due to subscription termination or nonpayment.

Therefore, a less granular approach to data ownership and an orientation towards the centrality of *control* over data will be adopted. Further clarifications are then needed. First, such authority tends not to be exclusively granted to solely one physical or legal person due to the two properties identified above. Second, data ownership is expressed by certain faculties which include the power of excluding others to enjoy a given piece of information or, conversely, to grant third parties the possibility to access, share and transmit data. Third, our definition is agnostic with respect to the concept of data at stake: it is applicable to all the meanings (e.g. personal, provided, inferred) of data identified in the previous subsection. Finally, nothing prevents other definitions (including legal ones, e.g. "data controller", "data subject", "right-holder") to apply contextually to "data owner".

3^{rd} working definition: Data Ownership

Bundle of control powers over data held by a physical or legal person, which might include the faculty of using, accessing, analysing, sharing, erasing, and transmitting digital information

1.2.5 Data Governance

This subsection aims to define a working definition for "data governance". As we have seen in the previous section, the property of data may originate numerous, co-existent ownership regimes over the same resource. Despite the natural tendency of data to be hardly excludable and not subtractable due to low reproduction costs, the co-existence of ownership models is not exempt from generating conflicts regarding the exploitation of informational resources, particularly in Big Data charcterised by high Value. This entails the necessity of regulating how information is managed, shared, accessed, analysed, and so forth. Hence, the need of identifying effective data governance frameworks capable of maximasing the benefits of Big Data.

In general, two major uses of "data governance" can be found in the literature and in common language. One is mostly associated with the idea of data "as-an-asset" held by private entities and it is heavily connected with business-oriented data analysis, storage, and use. Many different expressions describe the specific emphasis that data owners should put on data-related issues. "Data governance" is the branch of Enterprise Information Management (EIM) aiming at maximising data value by improving data quality (Ladley, 2012, p.7, p. 101). Similarly, Data governance has been defined as "the formulation of policy to optimize, secure, and leverage information as an enterprise asset by aligning the objectives of multiple functions" (Soares, 2015). Synonyms also include "data quality management" (Wende, 2007). Data governance "models" have been drafted starting from the level of maturity of a private entity towards data and organised in steps (The Data Warehousing Institute, 2013). IBM (Firican, 2018), Oracle (Oracle, 2013), and Gartner (Gartner, 2008) are popular examples of maturity-based data governance models.

The second definition of "data governance" is less focused on the operational use of data by companies and more keen on discussing "all processing of governing" (Bevir, 2012) "Governance" derives from the Greek κυβερνάω (to steer) and this second meaning reflects the one originally conferred by Plato in his *Republic*. Thus, it transcends the traditional meaning of State, law, government and can be identified as the set of decision-making processes within a community. Such processes encompass governments, markets and networks, thus being a distinctive feature of multi-stakeholder environments. 'Hard' law is not the only governance tool: hybrid practices often combine administrative systems with market strategies and no-profit arrangements (Bevir, 2012)[35]. As the following Chapters will discuss in detail, such mixed forms of governance also apply to ICT contexts (Pagallo et al., 2019).

In this second meaning, "data governance" has already been conveniently defined by several entities. A similar expression, "information governance" has been defined as "the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals." (Logan, 2010). Then, the Data Governance Institute has affirmed that "Data Governance is a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which describe who can take what actions with what information, and when, under what circumstances, using what methods." (The Data Governance Institute, 2015). Moreover, data governance has also been defined as "the formal execution and enforcement of authority over the management of data and data-related assets", "formalizing behaviour around the definition, production, and usage of data to manage risk and improve quality and usability of selected data" and "formalising and guiding behaviour over the definition, production, and use of information and information-related assets" (Seiner, 2014, p.2-3)[36]

The UK British Academy and the Royal Society have defined "data governance" in more holistic terms by including "legal, ethical, professional and behavioural norms of conduct, conventions and practices that, taken together, govern the collection, storage, use and transfer of data" (British Academy and Royal Society, 2017). This definition looks appropriate for the context of this dissertation. Its major advantages consist of reconciling ethical norms and rules, defining certain types of data processing, and including practices among the component of data governance[37].

[35] For an extended discussion on the concept of governance, the eight definitions reviewed by Grindle (Grindle, 2007) provide useful insights on its definition.

[36] Despite their linguistic similarity, the three definitions present a different focus: the first is mostly related to the exercise of control and authority over data-related decision-making processes; the second is focused on enhancing data quality; the third is more concerned by the procedural aspects of data management.

[37] However, the lack of "erasure" among the inspected types of processing has to be noted con-

To summarise, this subsection has identified two meanings of data governance, the former describing the management of informational assets to improve quality and maximising profits, the latter being focused on the allocation of powers, rights and responsibilities of data processing by means of legal, ethical and behavioural rules. In this dissertation, the second meaning of data governance will be preferred consistently with our focus and due to the presence of multiple entities (e.g. food safety authorities, food business operators, consumers), conflicting interests and the need of holistic solutions.

4th working definition: Data Governance

Legal, ethical, professional and behavioural norms, convention and practices that, taken together, powers, rights and responsibilities for the collection, storage, deletion, use and transfer of data.

1.3 Research Question

The section below identifies the research question of this dissertation and three sub-questions that will be discussed throughout its Chapters.

Sub-questions represent specifications of the main research question that pertain to three directions of investigations, or areas of research. While sub-questions are, by definition, subordinated to the main research question, the value of each sub-question is equal to the others. Moreover, they should be considered intertwined and mutually dependent, rather than isolated.

Research Question

How can data ownership and data governance be shaped to maximise the benefits and minimise the risks of using and processing Big Data in the context of EU Agri-Food safety risk assessment?

As explained in the following section on research methodology, the dissertation aims to identify a set of ethical principles that can inspire solutions for ownership and governance issues that could prevent the fulfilment of Big Data's positive impact in agri-food safety risk assessment. The answer to the main research question will be provided through a "Roadmap", i.e. a practical guide aimed at offering

sistently with what has been observed in the previous section. We will assume that a very broad interpretation of "storage" includes both retention and deletion of data high-level recommendations for the implementation of such principles.

1.3.1 Technology: How Big Data reshape ownership and governance

The first sub-question investigates the technical challenges of Big Data, in particular by focusing on peculiarities that significantly impact data ownership and data governance in the domain of agri-food safety. *Inter alia*, a practical example is the trend that involve the creation and the analysis of mixed datasets for risk prediction purposes. It is possible that different ownership models co-exist within the same dataset or - as it has already been noted - that governance frameworks change according to the legal type of data at stake. Moreover, issues pertaining to ownership and governance of derived or inferred data are likely to require a specific enquiry. This and similar questions need special attention from a technological viewpoint. Posing technical questions in first place helps us to discuss ethically-oriented solutions consistently with the technicalities of the data processing at stake, in particular to avoid detached, attainable or impossible results.

1st Research Sub-Question

How are data accumulation, transmission and analysis reshaping ownership and governance of data in the agri-food safety domain?

1.3.2 Ownership: Property rights, transparency and data protection

The complexity of agri-food safety Big Data systems is reflected in balancing ownership rights when multiple and conflicting interests are at stake. For instance, the simultaneous presence of non-personal, company-owned data and personal information within mixed datasets raises questions about what kind of control powers individuals and authorities should be entitled to exercise. Moreover, the call for a more transparent risk assessment has been quite recently transposed in an EU Regulation, and the implications regarding the balance between transparency and preserving a competitive environment for the agri-food industry are yet to be discussed.

2nd Research Sub-Question

How is it possible to balance the need of property rights emerging from agri-food industry, the calls for more transparency coming from public society and rights over personal data?

1.3.3 Governance: Data governance models and values to be embedded

Among our research areas, data governance has perhaps the broadest scope. Therefore, it is necessary to identify a narrow research sub-question that is consistent with the general and ethically-oriented research goal of this dissertation and with the latest advances in research methodologies on data governance. A position recently taken by some scholars correctly points out the increasing complexity of technological regulation recommends new models of governance and how such models should also be based on the interplay of law and other regulatory systems, such as forces or the market, or social norms (Pagallo et al., 2019). Most importantly, this position seems correct when identifying legal governance as a twofold process in which rules, principles and values enable regulatory systems to encompass legal instruments, and conversely the representation and the implementation of legal systems can occur through formal languages, machine-learning algorithms, NLPs and computational ontologies[38]. In answering the following question, we will mostly focus on the first area of research and leave the second one to be discussed in further studies.

3rd Research Sub-Question

What rules, principles and values should be reflected into the data governance models and frameworks that regulate the behaviour of the entities involved in EU agri-food safety risk assessment?

[38] In the cited paragraph of their paper, Pagallo and colleagues (Pagallo et al., 2019) discuss the Web of Data. While the complexities of linked data systems present unique challenges that are out of the scope of this dissertation, their operational description of legal governance seems appropriate for this thesis and consistent .

1.4 Research Methodology

A more detailed account of our research methodology is given in the following section. It has to be observed that, given the diversity of topics and research questions covered by this dissertation, the interdisciplinary approach of legal informatics (Sartor, 2016) has been adopted[39] jointly with data ethics (Floridi and Taddeo, 2016)

Figure 4 portraits the chosen methodology, while the following subsections describe each step.

The Roadmap presented in Chapter 6 has been drafted starting from principles identified among those pointed out in "ethical charters" (e.g. the work done by the EU Commission High-Level Expert Group (HLEG)), which in turn have been drafted on the basis of principles enshrined in the field of data and information ethics. However, these charters purposively cover a wide range of topics, applications and practices, and some of their governance recommendations could not be appropriate for the realm of agri-food safety risk assessment.

The high generalisability of the ethical charters originates the need of adapting these documents and their principles (also discussed in light of contributions in information and data ethics) to the domain discussed in this dissertation. The context of agri-food safety risk assessment has been constructed by following a bottom-up approach (fig. 1.4). Food safety risk assessment is conceptualised as a:

1. a technical domain, i.e. data processing activities carried out when assessing food safety risks, and

2. a legal domain, i.e. EU legislation, the jurisprudence of the European Court of Justice and academic commentaries discussing governance and ownership issues related to food safety.

to which high-level ethical findings shall be applied.

[39] In his own words (p. 40-41): "Information technologies concur to determine possible legal advances: new norms should both prescribe behaviours that are technically possible and choose (within the margin of manoeuvre granted to the Legislator) those which better suits political and legal values to pursue. [...] The sphere of what is technologically (*rectius*, informatically) feasible encompasses both what our society is (i.e. existing structures and current behaviours) and what is can become (risks and opportunities); *de jure condito* normativity and *de jure condendo* normativity regard behaviours (reality, risks and opportunities) to be framed within this sphere. (*ED.* author's own translation. Original language: Italian)"

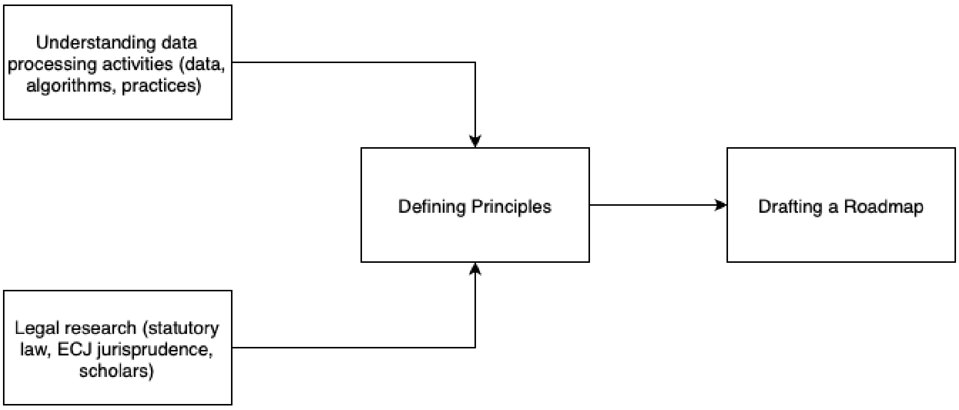

Understanding data processing activities (data, algorithms, practices)
Defining Principles
Drafting a Roadmap
Legal research (statutory law, ECJ jurisprudence, scholars)

Figure 1.4: Research Methodology

1.4.1 A qualitative assessment of Big Data applications and methods

The identification of applications that rely or use Big Data in the context of agri-food safety is the first step to define a technical framework for further analysis. This has been done through a 2-step process. First, a descriptive literature review, whose results are discussed in Chapter 2, has been performed to assess the presence of research trends and methodologies that use large quantities of data in food safety risk-related scenarios. The literature discovery was not aimed to identify research gaps or critically discuss research findings. Instead, it has been used as a preliminary step for a qualitative assessment of these applications necessary to identify elements that can be helpful in preparation of the ethical analysis.

Following this research, the review phase has been aiming to the identification of "clusters" or "families" of algorithms according to the taxonomy provided by Kantardzic (Kantardzic, 2011) reported above (§1.2.3). The reason underlying this choice is threefold: (i) to assess if Big Data practices are popular in agri-food safety risk assessment, (ii) what algorithms are used for the analysis and (iii) for what purposes they are deployed.

Following the threefold goal of identifying theoretical or practical contributions in the technical perspective of the research topic, the keyword selection has included "Big Data", "Machine Learning" and "Artificial Intelligence". This choice is the frequent use of these expressions as equivalent and the possibility of linking resources given by databases containing papers and citations. The use of broad terms, moreover, should enlarge the spectrum of algorithms and data types at stake[40]. These

[40] Consistently with the given technical definition of data, inferential processes have to be kept

keywords have been linked to "food safety" and "EFSA". The former string has been also narrowed to "Risk Assessment", while the latter has been made explicit in "European Food Safety Authority".

Table 1.3: Literature Search - String selection

Technical Term	**Domain**	**Specification**
Big Data	Food Safety	Risk Assessment
Machine Learning		
Artificial Intelligence	EFSA	European Food Safety Authority
Data Mining		

Following keyword selections, 12 research queries were created. Fixed quotation marks ("") have been used when querying the database in order to "fix" expressions like "Big Data" or "Artificial Intelligence", in a manner that they appeared always in pair[41]. Even though it was possible to specify research queries by including algorithms or practices (e.g. "K-means clustering" or "Neural networks"), specific terms were not included in the literature research to avoid some kind of pre-selection of algorithms and methods.

Web Of Science and Scopus have been selected due to their advantages. On the one hand, Web of Science provides detailed citation analysis tools, which is crucial for an accurate detection of research trends. On the other hand, Scopus covers a wider spectrum of journals (Falagas et al., 2008). Web of Science has been explored using the "TOPIC" filter, which includes title, abstract, author keywords, and Keywords Plus[42] of the paper. Similarly, Scopus results have been filtered by article title, abstract and keywords. Then, a .CSV table containing uniquely identified journal articles and their citations have been created to identify and remove duplicates[43]. The table below summarises the results of the literature search and displays the "raw" number of unique papers extracted from the databases.

into account. The possibility of obtaining high quality derived and inferred data through analytical techniques such as Machine Learning requires the adoption of a "dynamic" approach to Big Data, rather than confining the exploration of the literature to the "static" aspects of Big Data, such as accumulation or storage

[41] A first round of literature search was performed using individual Boolean expressions rather than quotation marks (e.g. Big AND Data instead of "Big Data"). Despite the increase in document retrieval, the quality of the retrieved papers was dramatically low. For instance, the inclusion of "mining" together with "risk" generated a stunning number of useless results related to the risks associated with coal and mineral extraction.

[42] KeyWords Plus are a unique feature of Web of Science and consist of words and phrases automatically extracted from the titles of articles in the retrieved paper.

[43] 21 papers were also excluded from the review for not being available in English

Table 1.4: Literature Search - Results

String	**Web of Science** (TOPIC)	**Scopus** (Abstract, Title, Keywords)
"Big Data" AND "Food Safety"	41	57
"Big Data" AND "Food Safety" AND "Risk Assessment"	7	29
"Big Data" AND (EFSA OR "European Food Safety Authority")	3	2
"Machine Learning" AND "Food Safety"	37	57
"Machine Learning" AND "Food Safety" AND "Risk Assessment"	2	3
"Machine Learning" AND (EFSA OR "European Food Safety Authority"	2	3
"Artificial Intelligence AND "Food Safety"	9	69
"Artificial Intelligence" AND "Food Safety" AND "Risk Assessment"	2	3
"Artificial Intelligence" AND (EFSA OR "European Food Safety Authority")	2	3
"Data Mining" AND "Food Safety"	5	76
"Data Mining" AND "Food Safety" AND "Risk Assessment"	32	9
"Data Mining" AND (EFSA OR "European Food Safety Authority")	2	1
Total	144/(**112** unique)	312/(**140** unique)

1.4.2 Legal Research: statutory law, CJEU jurisprudence and academic commentaries

Another key component of the methodology consists of legal research. As for the technical background of this thesis, this subsection aims to discuss what steps have been taken in the identification of legal sources. Our general assumption is that EU agri-food safety risk assessment regulation is a set of norms being part of a legal system. Ontologically speaking, we rely on the antiformalistic construction operated by Pattaro and his definition of norms as "deontic propositional content believed by at least one person to be normative" (Pattaro et al., 2005, Ch. 6).

As Sacco argues (Sacco, 1991), no statement of the law is complete or fully accurate. Various versions of the norms or "legal formants" are subject to different interpretations. Such formants consist of statutory law, case law and academic commentaries. Two clarifications are necessary. On the one hand, Sacco identifies the presence of formants while discussing the methodological paradigms of legal comparison, a methodology that will not be followed in this dissertation. However, his description will be used as a guideline to identify the peculiarities of the legal system under scrutiny rather than, for instance, to identify "criptotypes" - or hidden meaning of laws - by comparing legal systems, as he argues. On the other hand, his description of a "legal system" may seem to operate at a very high level of abstraction. Hence, it is important to contextualise the legal system under scrutiny to the narrow set of norms, cases and journal articles according to the criteria reported below.

In Chapter 3, EU food safety law has been described first from an historical perspective, from its origin in 1997 to its latest reform in 2019. In particular, our focus regards provisions regulating openness and transparency of data. Three sectoral legal frameworks (Genetically Modified food and feed, health claims, and novel foods) have been individually assessed due to the contextual presence of conflicting interest and relevant ethical challenges. Similarly, statutory law regarding the protection of personal data - limited to certain key definitions and the rationale underlying the entry into force of the GDPR - and non-personal data - in particular the provisions regarding the free flow of data and the Database Directive as the general legal context for data ownership and governance - have been taken into account.

Case law consists of rulings of the Court of Justice of the European Union (CJEU), regarding crucial aspects of openness of data used in the food safety risk assessment and the careful balance between transparency of environmental information, free flow of data and rights over personal data. The CJEU jurisprudence taken into account was also previously reviewed by legal scholars and policy makers.

Finally, academic commentaries have been selected among contributions discussing food safety risk assessment within broader contexts, such as data ownership, competition in market sectors that rely on big data and policy-making related to personal and non-personal data. The broader scope of academic commentaries is crucial to bridge the gap with data governance that, as we have seen, understands norms of conduct in broader terms than statutory or case law.

1.4.3 Contributions in information and data ethics

As mentioned above, a preliminary assumption is that information and data ethics (Floridi and Taddeo, 2016) can provide guidance to draft the principle-based Roadmap that constitutes the product of this research. Contributions in information and data ethics are needed every time a data-related ethical dilemma - i.e. choosing between two or more possibilities that, in principle, are equally right (or equally wrong) - emerges[44]. As it will be noted, the emergence of ethical dilemmas is quite common

[44] This likely controversial statement shall be clarified. If data ethics is contextualised as one of the emergent fields of applied ethics, it follows that it inherits all the advantages and disadvantages of this category. In particular, in his review of critical approaches to applied ethics, Fossa (Fossa, 2017) noted that some philosophers struggle to recognise it as a serious philosophical discipline due to an alleged lack of rigorousness and the possible hybridisation of moral philosophy and professional practices. However, we agree with the Author when he also notes that "application, in ethics, has primarily to do with the reasons that give moral meaning to our behaviours". Such behaviour,

in this domain. The task of data ethics is to maximise the "ethical value of data science to benefit our societies, all of us and our environments".

Methodologically speaking, Floridi and Taddeo clarify that the role of computer, information and data ethics by highlighting their different level of abstractions (LoA)[45]. While LoA$_I$ (the LoA of information ethics) is mostly information-centric, the LoA$_D$ (the LoA of data ethics) is clearly data-centric. While "the shift from information ethics to data ethics is probably more semantic than conceptual" (Floridi and Taddeo, 2016), a specific focus on the moral dimension of data is undoubtedly convenient for the purposes of this dissertation. However, as information ethics (Floridi, 2006) is one of the forerunner of data ethics, contribution in this domain will be taken into account[46].

LoA$_I$ and LoA$_D$ differ under some perspectives. LoA$_I$ sets as observable the different moral dimensions of information when it is a source, the result or the target of moral actions. Hence, the modelling, sharing, retention, protection, use and deletion of information constitute possible variables of LoA$_I$. Data ethics and LoA$_D$ are focused on three different sets of intertwined moral problems, namely those related to "data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence, artificial agents, machine learning and robots) and corresponding practices (including responsible innovation, programming, hacking and professional codes)" (Floridi and Taddeo, 2016).

contextualised by the Author in terms of hermeneutic experience (in turn derived from Aristotle's practical philosophy), reflects morally-oriented solutions to problems occurring in practice. Hence, Fossa's hermeneutic theory of applied ethics is an attempt to reconcile moral philosophy and applied ethics.

[45] Floridi (Floridi, 2008) illustrates the method of abstraction. This methodology is widely used both in computer science and in philosophy and ethics of information and it is based on the identification of a Level of Abstraction (LoA), i.e. a "level" at which a system can be analysed, by focusing on different aspects, called observables, chosen according to the goals of the analysis. Any given system can be analysed at different LoAs. As he specified elsewhere (Floridi and Taddeo, 2016), "an engineer interested in maximizing the aerodynamics of a car may focus upon the shape of its parts, their weight and the materials. A customer interested in the aesthetics of the same car may focus on its colour and on the overall look and may disregard the shape, weights and material of the car's components"

[46] Instead, the perspective of Computer ethics (Moor, 1985), an other forerunner of data ethics, will not be discussed. The reason underlying this choice lies on the difficulty of framing LoA$_C$ within the scope of this dissertation, which is limited in terms of understanding the impact of computing in the society and in the environment, that is the goal of LoA$_C$

1.4.4 From principles to an ethical Roadmap

As previously remarked, this dissertation aims to draft a principle-based Roadmap for a trustworthy innovation in the field of data-based food safety risk assessment, in particular in the areas of data ownership and data governance. This attempt has to be read in conjunction with other documents issued by several entities (e.g. authorities, regulators, associations) that promote ethical behaviours in correlation with certain technologies using Big Data[47].

"Ethical charters" include a wide spectrum of recommendations, covering both technical solutions and legal, ethical and societal issues. For instance, in the work done by the group "AI4People"[48] An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations (Floridi, Cowls, et al., 2018), proposals are addressed to policy-makers and technicians according to a holistic, collaborative, and multi-stakeholder regulatory approach.

The methodology adopted by the AI4People Ethical Framework - as well as the one chosen in other "charters" - present advantages and disadvantages. On the one hand, they tend to put emphasis on the role of principles and values in determining certain morally-oriented recommendations. This method relies on investigating the literature to find principles on which a certain level of agreement has been reached (*cf.* Chapter 4 of the AI4People Ethical Framework (AI4People, 2018)) and thus grounding recommendations on such shared values; on the other hand, most of these ethical charters - including the AI4People Ethical Framework - are attempts to identify cross-sectoral, high-level and *one-fits-all* morally-oriented solutions. This entails that, despite the high consensus achieved among communities of experts, technicians and policy-makers (OECD, 2019), these frameworks still have to be applied and adopted in real-world applications (Floridi, 2019a). It is likely that implementations and interpretations - like the one proposed in our Roadmap - would be needed to "fit" ethical frameworks within domains affected by peculiar risk factors or bringing new opportunities.

As argued thus far, our domain (ownership and governance) is methodologically constrained by technical and legal boundaries. Hence, the proposed recommenda-

[47] It worth noting that the proliferation of these initiative might be a consequence of the emerging concerns related to the increasing use of Artificial Intelligence techniques. However, this does not entail that these documents could not fruitfully used in a "Big Data" context given that AI notoriously demands large quantities of structured and high quality data to deliver satisfactory results. More on this topic will be discussed in the Chapter 2

[48] AI4People is a multi-stakeholder forum, bringing together all actors interested in shaping the social impact of new applications of AI, including the European Commission, the European Parliament, civil society organisations, industry and the media(AI4People, 2018)

tions - i.e. our ethical Roadmap[49] - will be drafted by taking into account what is technologically and legally feasible according to the principle *"ad impossibilia nemo tenetur"*.

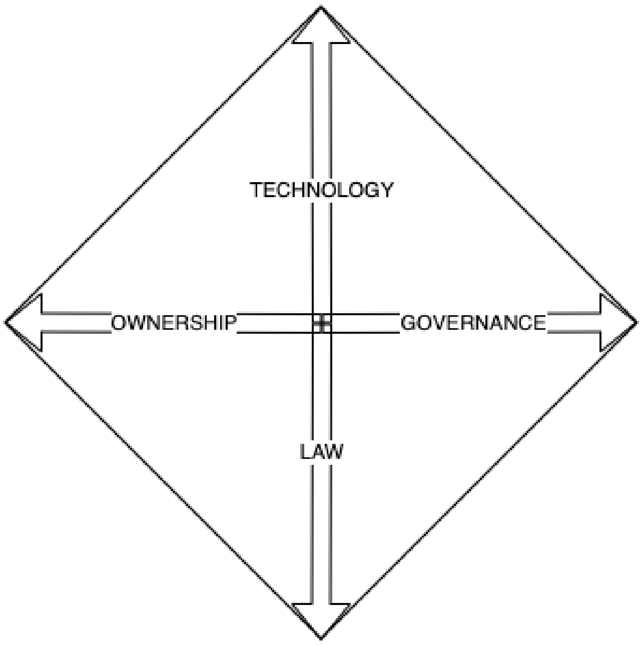


Figure 1.5: Research scope of the dissertation

1.5 Outline of the thesis

Following this Introduction, this dissertation contains 5 Chapters.

Chapter 2 shows the outcome of the qualitative assessment of Big Data applications, methods and practices (**§2.2**, **§2.3**) deployed in the context of agri-food safety risk assessment. The discussion in **§2.4** identifies the presence of three intertwined informational elements of risk assessment, i.e. personal, non-personal and mixed data. If compared to other domains where only one component can be found, the contextual presence of these components emerges an element of novelty.

Chapter 3 analyses the agri-food safety risk assessment legal framework from the

[49] The name "Roadmap" has been preferred to be distinguished from the terms "Guideline" (which evoke of some kind of regulatory power), "Framework" (which - by definition - needs to be filled with some kind of "content" that is adapted to the container, whereas this dissertation aims to be the substance filling an already established framework), and "Charter" (which might originate confusion due to its frequent use in the context of international law)

perspective of the three formants identified above. In particular, following the introduction of the General Food Law Regulation (GFLR) (**§3.1**), a discussion on the new EU Regulation 2019/1381 ("Transparency Regulation") amending the GFLR is presented, followed by highlights on three sectoral regulation (**§3.2**), recent advances in CJEU jurisprudence (**§3.3**) and specific issues linked to openness, transparency and trust in light of the question of data ownership, as well as foreseeable legal challenges (**§3.4**).

Chapter 4 adopts an ethical perspective and discusses the principles underlying the Roadmap. On the one hand, **§4.1** introduces the necessity of ethical contributions in this domain and identifies what kind of background principle should be necessary. **§4.2** examines the principles enshrined in the institutional charters and supplementary papers, whereas **§4.3** critically evaluates some alleged methodological pitfalls and proposes solutions to adapt these framework to the technical and legal domain framed in Chapter 3 and 4.

Chapter 5 presents the practical product of this dissertation, i.e. the ethical Roadmap for Big Data analysis and processing in the context of food safety. Following an introduction on the objective and the scopes of the Roadmap **§5.1**, the P-SAFETY model is presented in **§5.2**. Possible implementations are briefly discussed in **§5.3**

Finally, the conclusive **Chapter 6** presents a synopsis of the thesis in **§6.1**, which mirrors the research questions presented in the introduction. Then, **§6.2** illustrates the significance of this study. Limitations and possible directions for further research are discussed in **§6.3**

An **Appendix** displays some relevant tables to which occasional references are made. A chapter-by-chapter **Bibliography** is presented at the end of the dissertation.

2

Data analysis practices in the context of EU food safety risk assessment

2.1 Data-based food safety risk analysis in the EU

Consistently with our research question and research methodology, this Chapter aims to discuss some technical aspects of Big Data practices in EU food safety risk assessment. As stated above, data are becoming a valuable resource in the performance of risk assessment activities carried out by EU authorities. This Chapter explores consolidated and emerging data gathering and analysis techniques in order to bridge the gap with legal and ethical considerations related to the use of these data. For descriptive purposes, this Chapter first distinguishes data "sources" and data "analysis" techniques for risk assessment, then discusses technical findings from a broader perspective to link this evidence with other parts of this thesis.

As stated above, risk assessment is part of the broader concept of risk analysis (fig. 1.1), which also involves risk management and risk communication. Interestingly, the EU is actively promoting data-related initiatives in the other fields. While an in-depth analysis of these advances is out of the scope of this paper, a few remarks about them might useful for comparison.

On the one hand, risk management has recently introduced the Information Processing System for Official Controls (IMSOC) within the Official Controls Regulation[50]. The Commission is now in charge of creating and maintaining a digital repository containing "data, information and documents concerning official controls" on food and feed entering the EU market. Therefore, these activities are "managed, handled, and automatically exchanged" (art. 133 of the Official Controls Regulation). Since the Commission was also demanded to implement the system according to the guidelines provided by Art. 134 of the Official Control Regulation, it enacted the Implementing Regulation 2019/1715[51]. The new system encompasses iRASFF, ADIS, EUROPHYT, and TRACES, four databases containing information regarding foods, animals and plants that circulate within the Union. Thanks to the information stored in new database, the new system will also assist competent authorities in Member States to assign a rating to food business operators on the basis of criteria published by competent authorities (Art. 11(3)(a)). This complex database will also be the base of predictive analysis[52].

On the other hand, risk communication has been oriented towards a twofold goal. First, the Rapid Alert System for Food and Feed (RASFF) provides two portals (RASFF Portal[53](fig. 1.2) and RASFF Consumer Portal[54]) containing and displaying notifications pertaining to food recalls from the market. Pages are freely searchable and data can be downloaded in XML format, free of charge and without registration. Despite the informative nature of the dataset, researchers (Bouzembrak and Marvin, 2019) have used these data to predict safety hazards and food frauds.

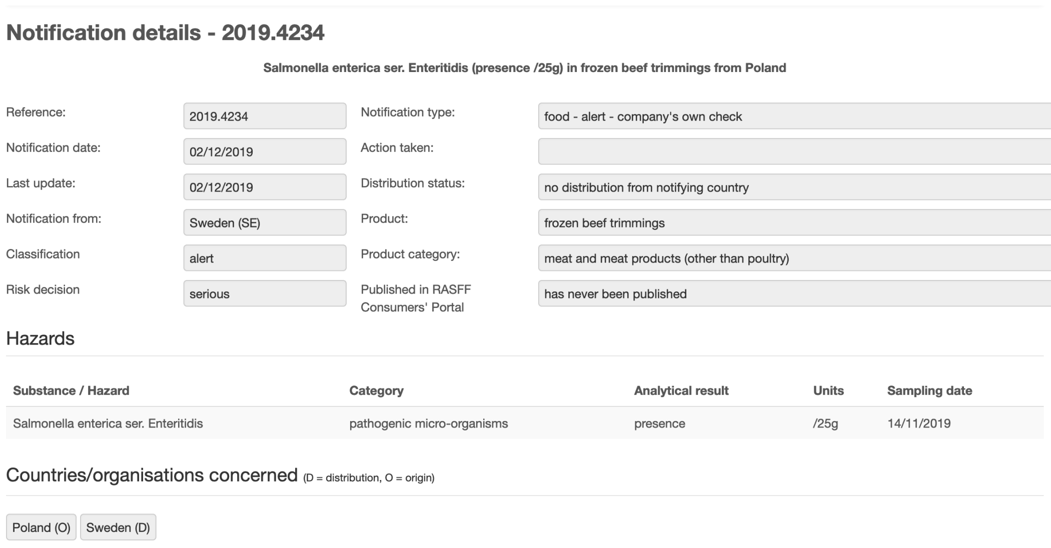
[50] Regulation (EU) 2017/625 of the European Parliament and of the Council of 15 March 2017 on official controls and other official activities performed to ensure the application of food and feed law, rules on animal health and welfare, plant health and plant protection products, amending Regulations (EC) No 999/2001, (EC) No 396/2005, (EC) No 1069/2009, (EC) No 1107/2009, (EU) No 1151/2012, (EU) No 652/2014, (EU) 2016/429 and (EU) 2016/2031 of the European Parliament and of the Council, Council Regulations (EC) No 1/2005 and (EC) No 1099/2009 and Council Directives 98/58/EC, 1999/74/EC, 2007/43/EC, 2008/119/EC and 2008/120/EC, and repealing Regulations (EC) No 854/2004 and (EC) No 882/2004 of the European Parliament and of the Council, Council Directives 89/608/EEC, 89/662/EEC, 90/425/EEC, 91/496/EEC, 96/23/EC, 96/93/EC and 97/78/EC and Council Decision 92/438/EEC (Official Controls Regulation)[2017] OJ L 95

[51] Commission Implementing Regulation (EU) 2019/1715 of 30 September 2019 laying down rules for the functioning of the information management system for official controls and its system components (the IMSOC Regulation) [2019] OJ L 261/37)

[52] Commission Staff Working Document accompanying the document Report from the Commission to the Council and the European Parliament - Second Progress Report on the implementation of the EU Strategy and Action Plan for Customs Risk Management, p. 40

[53] https://webgate.ec.europa.eu/rasff-window/portal/?event=SearchForm&cleanSearch=1

[54] https://webgate.ec.europa.eu/rasff-window/consumers/



Notification details - 2019.4234

Salmonella enterica ser. Enteritidis (presence /25g) in frozen beef trimmings from Poland

Reference:	2019.4234	Notification type:	food - alert - company's own check
Notification date:	02/12/2019	Action taken:	
Last update:	02/12/2019	Distribution status:	no distribution from notifying country
Notification from:	Sweden (SE)	Product:	frozen beef trimmings
Classification	alert	Product category:	meat and meat products (other than poultry)
Risk decision	serious	Published in RASFF Consumers' Portal	has never been published

Hazards

Substance / Hazard	Category	Analytical result	Units	Sampling date
Salmonella enterica ser. Enteritidis	pathogenic micro-organisms	presence	/25g	14/11/2019

Countries/organisations concerned (D = distribution, O = origin)

Poland (O) Sweden (D)

Figure 2.1: RASFF Portal

Secondly, EFSA (@EFSA_EU), its thematic departments (@Animals_EFSA, @Methods_EFSA, @Plants_EFSA), the EU Commission's Directore General responsible for food safety, Health and Food Safety (SANTE) (@EU_Health) are active on Twitter.

Regarding risk assessment, several data-related programs are currently run by EFSA in the area of Big Data sources, while advanced data analysis techniques (including predictive algorithms) are still undergoing research. A short position paper entitled "The Future of Data in EFSA" (Cappè et al., 2019) was released by EFSA in early 2019. Data landscape for the future was defined by the Authority as "the forefront of our thinking" and several advancements in data-based food safety risk assessment were presented. In their words, the Authors stated that "we are looking into novel information streams, crowd-sourcing, real-time monitoring systems throughout the food chain, "Internet of Things", combining standards to improve data exchange capability and much more to ensure we create a growing pool of large, complex scientific data sets accessible with minimal manual intervention".

The first goal of this chapter is to identify these key initiatives within EFSA, already summarised by the literature (Alemanno and Gabbi, 2016, p.79) then to look at what the future of food safety data analysis at EFSA might look like. The Authority has also stated that Artificial Intelligence and Big Data represent an opportunity to "increase efficiency (in terms of time and human resources) in the data-to-evidence process (search, appraise, integrate)" (EFSA, Bronzwaer, et al., 2019).

At the same time, it is necessary to focus on ongoing trends regarding data analysis in food safety. As stated in the previous chapter, EFSA is in charge of reviewing data coming from the industry, thus having a direct contact with cutting-edge data analysis techniques. These methods may raise specific questions regarding, for instance, the transparency and opacity of algorithms or their impact on private life of individuals. Given the committent emerging from their papers, it is likely that the Authority will have to confront with these issues in the near future.

Sections **§2.2** and **§2.3** are purposively descriptive and aim to present technical evidence. Then, the legal and ethical implications of their findings are discussed and interpreted in section **§2.4**, where three informational components of risk assessment are identified. A short synopsis and critical issues to be discussed are then outlined in **§2.5**.

2.2 Big Data sources

This section identifies "Big Data sources" for food safety risk assessment. In particular, it covers both *strictu sensu* "data sources" (i.e. physical places where data originate) and platforms deployed to collect data across multiple sources to be used for further analysis (i.e repositories, databases, etc.). Following our definition, data at stake are mainly primary, provided and observed, whereas all the legal categories (personal, non-personal, mixed, etc.) are covered.

2.2.1 The EFSA Data Warehouse

The EFSA Data Warehouse has been built to become the main data source for risk assessment activities performed at EFSA (EFSA, 2011a). Data related to zoonotic diseases, antimicrobial resistance, foodborne outbreaks, pesticide residues, chemical contaminants, and chemical hazards collected yearly are accessible via this one-stop-shop hub. The database also contains data collected sporadically, i.e. *ad hoc* data collections derived from specific procurements (EFSA, 2015d). The goal of this initiative is to strengthen scientific progress by granting access to data to food safety professional, EFSA's stakeholders, and the general public.

EFSA Data warehouse is supported by access policies (Gilsenan, 2015) which formalise the levels of access and granularity of accessible data in precise rules (EFSA, 2015d). Access levels can be summarised as shown in the table below.

Table 2.1: EFSA Data Warehouse Access Rules

Level of Aggregation	**Accessible data**	**Entitled Users**
Low	All data needed to perform their duties	EFSA staff member and EU Commission (DG SANTE)
	All data needed to perform their mandates	Members of EFSA Penels and Scientific Committee (limited to the time necessary to perform their mandates)
Medium	Data provided by their own organisation	Data providers
High	Data presented by EFSA's scientific and technical outputs	Data providers (following EFSA's output)
		EFSA's stakeholders (NGO's, academia, national food safety authorities, etc.)
		General public

The granularity that defines the lowest level of aggregation is defined by EFSA in agreement with data providers and the European Commission. Therefore, it depends on the information-type at stake and might differ according to the stakeholders involved (e.g. academia, food business operators, etc.). Since Member States qualify as data providers, their level of access is limited to the amount of data that they provide. However, pilot studies on Member States that agree to share their data at a more granular level by entering in "Circles of Trust" have been conducted from 2014 to 2016 (EFSA, 2016b). The goal of these project is to strengthen knowledge sharing among Member States as regards laboratory practices, analytical methods and monitoring programmes.

As regards data collection, the majority of data in the area of occurrence of chemical and biological hazards is submitted to EFSA by national food safety authorities in EU Member Sates (Kocharov, 2009). Data providers also include food industry, consumer associations and the European Commission. EFSA also publishes continuous call for data[55] to further fill and keep updated its Data Warehouse.

[55] https://www.efsa.europa.eu/en/calls/data

2.2.2 EFSA Food Consumption Database

EFSA Food Consumption Database is the portion of the Data Warehouse that contains information on the amount of foods eaten by European citizens. While it follows Data Warehouse access rules, access to statistics is granted to companies willing of placing regulated products on the market and to the public[56].

EFSA has the right to use the raw, individual food consumption data for carrying out risk assessments and other scientific analyses. An authorisation from the data provider (usually, a Member State) has to be obtained prior to further processing of data. Summary statistics (high level of aggregation) from the Comprehensive Database are made available to the public on EFSA's website, and can be used by applicants submitting requests to place regulated products on the market to support their claims (EFSA, 2011a). The majority of occurrence data sent to EFSA comes from laboratories involved in national monitoring programmes and are submitted to EFSA by national competent authorities in EU Member Sates. Other data providers include the food industry (mainly via networks), universities, consumer associations, and the European Commission (DG SANCO). EFSA has established several data collection networks, composed of representatives of national competent authority data providers, to support its data collection activities in the field of food consumption data (Gilsenan, 2015).

The Comprehensive Database contains data characterised by high degree of granularity, both as regards food ingredients and individuals (EFSA, 2019b).

First, food consumption input data are classified according to the age of the individual consumer, the following population classes.

- Infants: $<$ 12 months old
- Toddlers: $\geq$ 12 months to $<$ 36 months old
- Other children: $\geq$36 months to $<$ 10 years old
- Adolescents: $\geq$ 10 years to $<$ 18 years old
- Adults: $\geq$ 18 years to $<$ 65 years old

[56] As Chapter 3 will discuss in detail, some food-related products - including GMOs, PPPs, additives, etc. - follow an authorisation process for which companies interested on their marketing shall go through. Since they are asked to submit data and evidence of safety to support their application, companies can make use of food consumption data to assess individuals' exposure to harmful agents and transmit their conclusions for EFSA's scrutiny

- Elderly: ≥ 65 years to < 75 years old
- Very elderly: ≥ 75 years old

After several pilot studies (e.g. PANCAKE (Ocké et al., 2012) and PILOT-PANEU (Ambrus et al., 2013)), the chosen methodology for all age groups (with the exclusion of infants and toddlers) is a 2-day non-consecutive 24-hour food dietary recall, i.e. a survey intended to gather data about the food and beverages consumed in the previous 24 hours (EFSA, 2014a). This interview might be self-administered or conducted by an expert. EFSA has reported that interviews last for 30 minutes on average. When the interview is carried out by a nutritionist, it consists of a computer-assisted personal interview (CAPI) or via telephone (CATI). Validated dietary softwares are used to carry out the survey, for instance to display pictures of foods to be chosen by the surveyed. Alternatively, picture books are used as visual supporting materials during the talk.

Background information including age, sex, marital status, region, rural/urban area, size of the household, household income, employment status are collected to detect dietary patterns. Instead, specific, predefined dietary patterns, whether through personal choice (e.g. vegetarians) or because of health conditions (e.g. diabetes or coeliac disease) are recorded. Finally, two measures (body weight and height) are directly used to perform exposure assessment (EFSA, 2014a, ch. 7). The full list of information collected is displayed in Table 4.4 in the Appendix.

Since 2019, foods are recorded as raw primary commodities (RPCs) (i.e. single units of unprocessed, harvested or slaughtered foods, like "apple"), RPC derivatives (i.e. processed RPCs, like "apple juice") and composite foods (i.e. foods consisting of multiple components, like "apple strudel") (EFSA, 2019b). Composite food consumption represents a unique challenge, as it has to be disassembled into RPCs. To do so, three tables are used. First, consumption data for composite foods (input data) are disassembled into RPCs and RPCs derivatives (intermediate data) using both the disaggregation table and the probability table. Then, processed RPCs are converted in RPC by a conversion table (output data).

The use of disaggregation table is meant to fragment composite food into derivative RPCs or RPCs. Hence, when a composite food has different flavours (e.g. type of muffin – chocolate or plain) or components (e.g. type of meat in a meatball), this table is also used to probabilistically assign such components. Composite foods components are manually entered into the the table by selecting the corresponding recipes (commercial products are indexed via Mintel Global New Products Database, while recipes are gathered from the website `allrecipes.com`). Then, a probability is calculated on a frequency indicator based on components' description.

Probability table, instead, is helpful to obtain more granular data. For instance, consumption records for vegetable oil will be assigned to a more specific oil type (e.g. sunflower oil, olive oil) based on probability on consumption of age classes (i.e. subjects < 1 year old, subjects ≥ 1 to < 10 years old and subjects ≥ 10 years old). This is expressed as a number ranging from 0 to 1.

Finally, conversion table translates quantities of RPC derivatives into their equivalent weight of RPCs before processing, i.e. the original ingredients. The conversion table is based on several papers and relevant literature, while no probabilistic method is involved.

Bulding the Comprehensive Database: a practical guidance
EFSA (EFSA, 2019b) reports the following example. For subjects aged ≥ 10 years, 2,215 individual consumption records were classified as "Pastries and cakes" in the Comprehensive Database. According to the probability table these consumption records may either be assigned to "Buns" (i.e. small pieces of sweet bread) with a probability of 50% or to "Sponge cake" with a probability of 50%. This has resulted in 1,100 of these consumption records assigned to Buns and 1,115 of these consumption records assigned to Sponge cake. The Comprehensive Database contained a consumption record where 175 grams of Sponge cake were consumed by an individual. According to the disaggregation table such Sponge cake is made of 26.1% egg, 24.5% wheat flour, 24.5% sugar, 24.5% butter and 0.4% baking powder. This has resulted in the following consumption records of 46.6g egg, 42.9g wheat flour, 42.9g sugar, 42.9g butter and 0.7g baking powder for the individual.

2.2.3 Standardisation initiatives: FoodEx2 and Standard Sample Description (SSD)

As we have seen when introducing exposure risk assessment and in the previous section, combining data on occurrence of micro-organisms and chemical contaminants or residues with food consumption data is crucial for risk assessment. It is thus necessary to consider harmonisation among organisations and entities participating food safety - a goal that EFSA has been pursuing since 2008 (Alemanno and Gabbi, 2016, p.88) - also in terms of technical interoperability. EFSA's Units managing databases need to receive, store and share data in a harmonised standard form (EFSA, 2011a).

Harmonisation goals have been conducted through standardisation initiatives. Two of them - FoodEx2 and Standard Sample Description - are briefly mentioned in this section to describe the efforts made by EFSA in harmonising various data coming from heterogeneous sources.

On the one hand, FoodEx2 is a food classification and description system aimed at harmonising data formats across different food safety domains and data providers. FoodEx2 allows matching food consumption and chemical occurrence data in order to perform exposure assessment (EFSA, 2015e). FAO and WHO are also using FoodEx2 to populate their databases (EFSA, 2018d).

FoodEx2 is structured hierarchically. Hierarchies represent different views on foods (and feeds) and they are are modelled according to the needs of the assessor. For instance, exposure hierarchy eases exposure assessment and food grouping. Overall, eight hierarchies are present in FoodEx2 revision 2;

- master hierarchy (entire terminology, for technical use only)
- reporting hierarchy
- exposure hierarchy
- pesticide residues hierarchy
- zoonoses hierarchy
- feed hierarchy
- veterinary drugs residues hierarchy
- botanicals hierarchy.

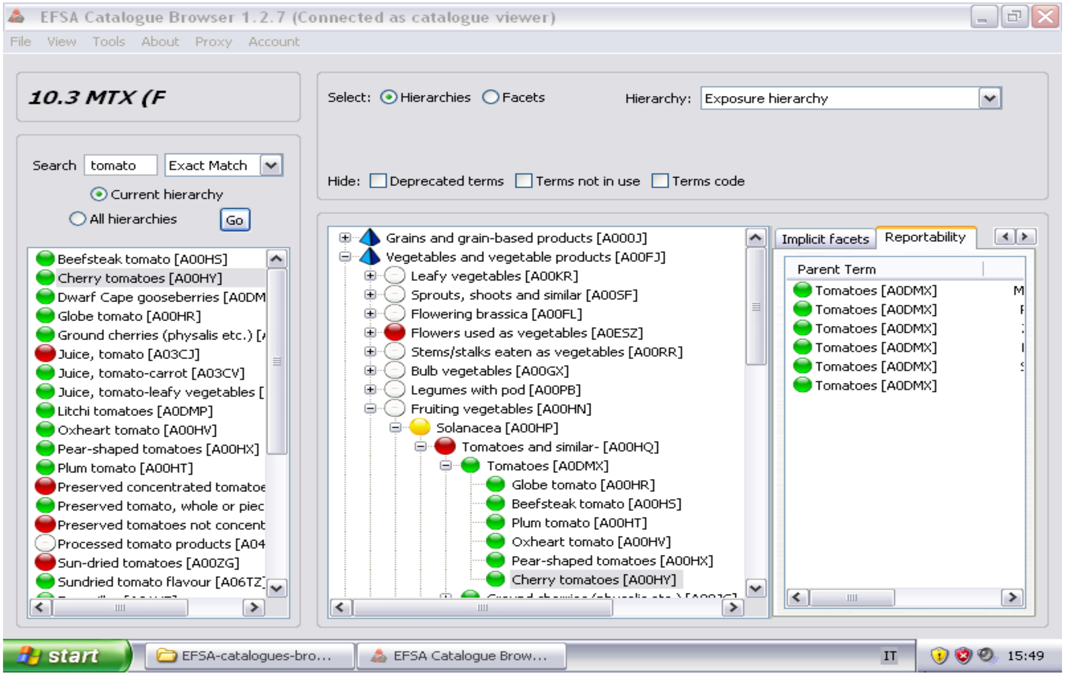
Exposure hierarchy is the preferred to report food consumption data. It is structured in six levels depending on the level of detail. It includes 4311 reportable terms, which correspond to the ones of reporting hierarchy. Each entry as an alphanumeric code uniquely associated to the term (A032 = "White Sugar"). For instance, EFSA (EFSA, 2015e, p.51) shows that the FoodEX2 code:

A042D#F04.A00QH$F04.A015L$F04.A00KV$F04.A00LN$F04.A00LB$F04.A00LG

equals to a common "mixed vegetable salad". The whole code should be read as follow: ingredient = carrots, ingredient = sunflower seeds, ingredient = Italian corn salads, ingredient = Roman rocket, ingredient = lollo rosso, ingredient = radicchio. As we have seen, probability table is used to disassemble composite foods into smaller units. In practice, the disaggregation allows the attribution of a FoodEx2 string to a composite food, as in the example reported above.

FoodEx2 browser is an open source catalogue published by EFSA, constantly updated (at least once per year). Information retrieval is performed with string matching and logic operators.

Results are shown according to the lowest possible hierarchical level that matches the query. Facets (i.e. descriptors such as packaging material and production method) and parent/child relations are also shown.



Search: tomato Exact Match

● Current hierarchy
○ All hierarchies

Select: ● Hierarchies ○ Facets Hierarchy: Exposure hierarchy

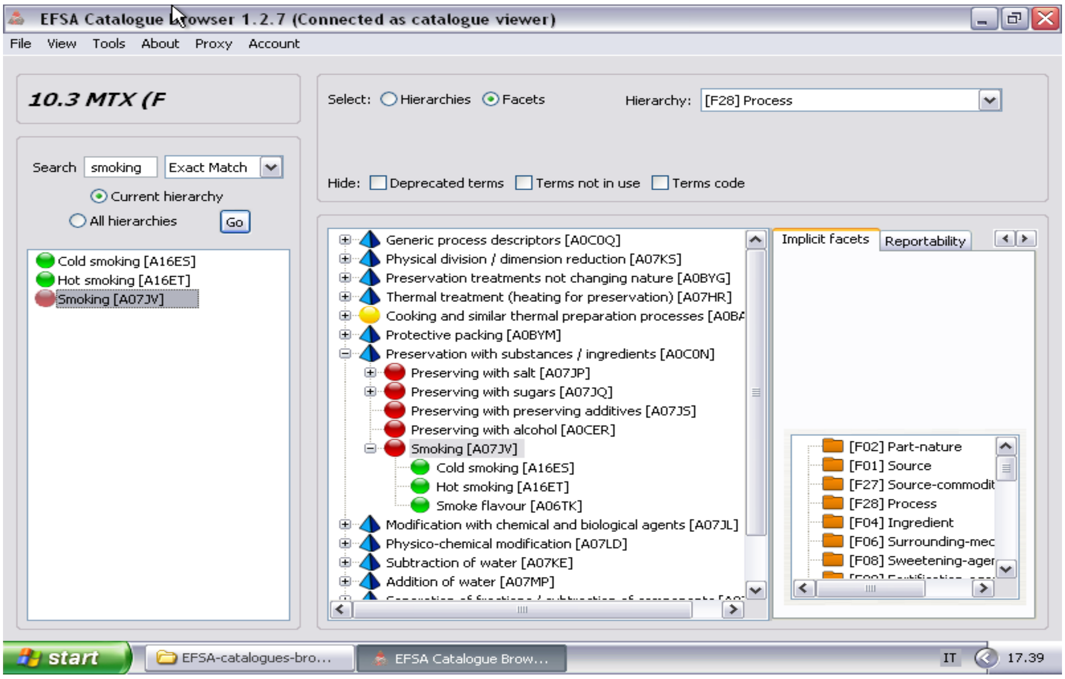
Hide: □ Deprecated terms □ Terms not in use □ Terms code

- Beefsteak tomato [A00HS]
- Cherry tomatoes [A00HY]
- Dwarf Cape gooseberries [A0DM
- Globe tomato [A00HR]
- Ground cherries (physalis etc.) [
- Juice, tomato [A03CJ]
- Juice, tomato-carrot [A03CV]
- Juice, tomato-leafy vegetables [
- Litchi tomatoes [A0DMP]
- Oxheart tomato [A00HV]
- Pear-shaped tomatoes [A00HX]
- Plum tomato [A00HT]
- Preserved concentrated tomatoe
- Preserved tomato, whole or piec
- Preserved tomatoes not concent
- Processed tomato products [A04
- Sun-dried tomatoes [A00ZG]
- Sundried tomato flavour [A06TZ]

```
⊞ Grains and grain-based products [A000J]
⊟ Vegetables and vegetable products [A00FJ]
    ⊞ Leafy vegetables [A00KR]
    ⊞ Sprouts, shoots and similar [A00SF]
    ⊞ Flowering brassica [A00FL]
    ⊞ Flowers used as vegetables [A0ESZ]
    ⊞ Stems/stalks eaten as vegetables [A00RR]
    ⊞ Bulb vegetables [A00GX]
    ⊞ Legumes with pod [A00PB]
    ⊟ Fruiting vegetables [A00HN]
        ⊟ Solanacea [A00HP]
            ⊟ Tomatoes and similar- [A00HQ]
                ⊟ Tomatoes [A0DMX]
                    Globe tomato [A00HR]
                    Beefsteak tomato [A00HS]
                    Plum tomato [A00HT]
                    Oxheart tomato [A00HV]
                    Pear-shaped tomatoes [A00HX]
                    Cherry tomatoes [A00HY]
```

Parent Term	
Tomatoes [A0DMX]	M
Tomatoes [A0DMX]	F
Tomatoes [A0DMX]	:
Tomatoes [A0DMX]	I
Tomatoes [A0DMX]	S
Tomatoes [A0DMX]	

Figure 2.2: FoodEx2 Browser. Research query: "tomato". Highlighted result: "Cherry tomatoes [A00HY]" in the Exposure Hierarchy (compatible with exposure assessment). Green dots represent the lowest possible level of detail



EFSA Catalogue Browser 1.2.7 (Connected as catalogue viewer)

10.3 MTX (F

Search: smoking — Exact Match

● Current hierarchy
○ All hierarchies

- 🟢 Cold smoking [A16ES]
- 🟢 Hot smoking [A16ET]
- 🔴 Smoking [A07JV]

Select: ○ Hierarchies ● Facets Hierarchy: [F28] Process

Hide: □ Deprecated terms □ Terms not in use □ Terms code

- Generic process descriptors [A0C0Q]
- Physical division / dimension reduction [A07KS]
- Preservation treatments not changing nature [A0BYG]
- Thermal treatment (heating for preservation) [A07HR]
- Cooking and similar thermal preparation processes [A0BA
- Protective packing [A0BYM]
- Preservation with substances / ingredients [A0C0N]
  - Preserving with salt [A07JP]
  - Preserving with sugars [A07JQ]
  - Preserving with preserving additives [A07JS]
  - Preserving with alcohol [A0CER]
  - Smoking [A07JV]
    - Cold smoking [A16ES]
    - Hot smoking [A16ET]
    - Smoke flavour [A06TK]
- Modification with chemical and biological agents [A07JL]
- Physico-chemical modification [A07LD]
- Subtraction of water [A07KE]
- Addition of water [A07MP]

- [F02] Part-nature
- [F01] Source
- [F27] Source-commodit
- [F28] Process
- [F04] Ingredient
- [F06] Surrounding-mec
- [F08] Sweetening-ager

Figure 2.3: FoodEx2 Browser. Research query: "smoking". Highlighted result: "Smoking [A07JV]" in the Process facet. Three specifications (Cold smoking, Hot smoking and Smoke flavour) are displayed at a lower level

On the other hand, Standard Sample Description (SSD) has been developed by EFSA to facilitate the exchange of analytical data on the occurrence of food-borne chemical and biological hazards (Gilsenan, 2015). It contains a list of standardised fields to be filled with information regarding samples, including the identification of the laboratory to which the sample belongs, the legal framework (especially in the case of national/EU monitoring programmes), the country of origin of the sample, the accreditation procedure for the analytical method, the accreditation of the laboratory, and the results. Outcomes are expressed in form of an XML code, such as `<evalCode> J003A </evalCode>`, which stands for "The residue in the sample is considered to be above the level of concern" (EFSA, 2019a, p.23).

Standardised data are then transmitted to EFSA via the Data Collection Framework (DCF). Accepted formats are Microsoft Excel, Comma-separated values (CSV) and XML (preferred by default). DCF also serves as data verification step, since it validates XML schemas for the transmitted document and reports error. Finally, data are further cleaned, stored and made available for analysis. (Gilsenan, 2015).

2.2.4 New trends in food-related data collection: IoT, smartphones, social media

The following subsection describes some emerging trends in data collection that are relevant to the domain of agri-food safety. As it will be shown, despite their effectiveness in other domains (Soon and Saguy, 2017), new approaches to food safety data collection have a moderate impact on risk assessment. This is due to multiple reasons, briefly discussed at the end of this section.

Internet of Things (IoT) can be broadly defined as artefacts capable of receiving and transmitting data via communication networks[57]. As a trend, the growing presence of IoT devices in several aspects of our lives entails several questions, including philosophical ones (Floridi, 2010, p.16), hence the need of briefly discussing to what extent IoT is reshaping food safety. EFSA has recently shown interested in IoT devices and information streams[58], consistently with research trends in the industry (e.g. as regards in-house food controls across the chain) (Jarschel et al., 2020).

The impact of blockchain on "smart" packaging and food traceability was briefly described elsewhere (Sapienza and Palmirani, 2018, para 4.2). Instead, a comprehensive literature review (Bouzembrak, Klüche, et al., 2019) has mentioned several studies on sensors used to collect humidity, temperature, and position data across the whole food chain. Communication protocols are often based on Internet, while radio frequency identifications (RFID) and wireless sensor networks (WSN) are the most frequent transmitting devices.

Despite the quantity of studies theorising IoT applications across the food chain, most of them look significant only for risk management, in particular since they allow for faster food recalls and securing data (Astill et al., 2019). Two Chinese studies show the potential of IoT devices in carrying out the monitoring of pesticide residue on the field. In the former (Jin et al., 2017), an IoT-based system collects data on pesticide residues directly from the field and transmit them to a food safety expert; in the latter (Zhao et al., 2015), consumers and food business operators can access the results of a monitoring IoT device by scanning a QR code. The predominance of Chinese studies described here and discussed in the aforementioned review (Bouzembrak, Klüche, et al., 2019) does not imply that foods coming from

[57] EU Commission Staff Working Document: "Advancing the Internet of Things in Europe", accompanying the document "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Digitising European Industry - Reaping the full benefits of a Digital Single Market COM(2016) 180"

[58] "We are looking into novel information streams, crowd-sourcing, real-time monitoring systems throughout the food chain,'Internet of Things' "(Cappè et al., 2019)

this region would not be available in the EU market[59]

Smartphones may have a significant impact on food consumption data gathering. Starting from EFSA Strategy 2020, the Authority has progressively endorsed the involvement of citizens through collaborative platforms and data crowdsourcing, both to foster trust in the Authority by engaging with citizens and to gather updated data. For instance, a 2017 EFSA tender (OC/EFSA/AMU/2017/02) asked participants to provide a “prototype design of a mobile app” to collect information pertaining to infants’ consumption data, alongside parents’ personal data regarding age, sex, region, size of the household, education, recent employment status and professional category.

Food consumption data gathered through memory-based methodologies (i.e. the traditional interviews and surveys described above) have been defined as "pseudo-scientific" by a highly critical research (Archer et al., 2015). Similarly (but with much less emphasis), Van den Puttelaar and colleagues (Van den Puttelaar et al., 2016) detected several disadvantages both for 24-hour food dietary surveys and questionnaires: long and time-consuming interviews, recall biases, likelihood in forgetting consumed food, and lack of contextualised information have been identified as the major drawbacks for dietary surveys.

One of the proposed solutions consists of using Internet and smartphones for dietary assessment, similarly to pivotal studies conducted in the USA in 2010 (Thompson et al., 2010). This approach is deemed to have the potential both to lower costs and burden and to facilitate a timely and accurate data analysis.

A good number of examples can be found in the literature. Authors (Van den Puttelaar et al., 2016) have modelled a mobile application - "FoodProfiler" - to overcome the aforementioned issues of memory-based methodologies. The mobile app proposes a 2-hour, self-executed and game-based food consumption recall. Other scholars have reviewed the use of publicly available apps for self-documenting food consumption (Eldridge et al., 2019), despite some remarks on the reliability, the quality and the interoperability of data for scientific uses (Maringer et al., 2018).

[59] They might fall under the scrutiny of EFSA under the "Novel Foods" regulatory framework - Regulation (EU) 2015/2283 of the European Parliament and of the Council of 25 November 2015 on novel foods, amending Regulation (EU) No 1169/2011 of the European Parliament and of the Council and repealing Regulation (EC) No 258/97 of the European Parliament and of the Council and Commission Regulation (EC) No 1852/2001 []2015] OJ L 327/1 - to which attention will be devoted in Chapter 3. The Regulation mandates EFSA to collect "scientific evidence demonstrating that the novel food does not pose a safety risk to human health" (art. 10.2(e)). In its Guidance on EFSA guidance for the preparation and presentation of applications for authorisation of novel foods, for instance, data pesticide residues have to be attached to the applications (EFSA, 2016a, para 2.4.1). In the near future, it is possible that data originated from IoT sensors would be submitted to EFSA according to such mechanism.

EFSA has seemed cautious in endorsing collaborative and smartphone-based methods, hence more research - outside the scope of this document - is needed to assess the validity of self-documented food consumption data collection. A general trend, instead, has to be noted. Despite EFSA's caution, single studies and extensive reviews show the promising results of these gathering methods to ease dietary intake assessment and data quality, especially in comparison to the methodologies currently in use by EU Member States competent authorities. In sum, despite being far from perfect, these methods could nonetheless provide significant benefits for dietary intake data gathering in the near future. This paradigm shift, however, is not exempt from significant concerns regarding the nature of the data at stake and discussed in section 2.4.1[60].

Gathering information from websites - in particular, social media - has been theorised as another crowdsourcing method (Marvin, Janssen, et al., 2017). Already in 2005, a study (Maeda et al., 2005) built a dataset of food-related hazards information from Google search results. "Web crawling" or "web scraping" approaches has been recently adopted to collect food consumption data on Instagram (Sharma and De Choudhury, 2015) and Twitter (Abbar et al., 2015), with the latter study being also focused on highlighting the concentration of obesity and diabetes. A similar study (Mejova et al., 2015) came to the conclusion that Instagram pictures (including metadata) were insufficient in generating a significant correlation with obesity, hence the proposal to include demographic knowledge in further research. Thanks to Instagram pictures, Phan and colleagues (Phan et al., 2019) studied alcohol consumption patterns over weekends.

Like IoT devices, the relevance of web scraping for food safety risk assessment is a general trend that has to be taken cautiously due to lack of consolidated methodologies. To date, no known study has been carried out by EFSA in this area, while third parties (in particular, academia and laboratories) have endorsed these research trends. Nonetheless, it is worth posing some questions regarding the legal and ethical implications of these methods as EFSA might receive data generated with novel methodologies or could opt to adopt these methods in the course of its own datafication transformation.

Instead, a few words have been spent by EFSA on supporting Emerging Risk Identification (ERI) with crowdsourced data. Social media, smartphone applications,

[60] An other crowdsourcing to be used for reference, smartphone-based solution supported and funded by EFSA is Mammal (https://mammalnet.com/collaborators/) project, which consist of a smartphone app (IMammalia) through which EFSA "will use collected information on abundance and distribution of wild mammals in order to assess the risk of diseases affecting wildlife, livestock, and humans". The collection of such user-generated information can be considered as part of the ongoing process aiming at fostering collaboration between the Authority and the general public, generating trust in EFSA and accessing update information with lower burdens

public health or economic indicators have been described as unstructured digital channels that require effort to be useful for information retrieval. Several challenges - including the identification of keywords and queries, the semantic relationship between linked data and visualisation of the results - have been identified (EFSA, Donohoe, et al., 2018). Further challenges might include the standardisation of data coming from different sources and the efforts needed to store and harmonise data gathered from smartphones or IoT devices within the EFSA's Data Warehouse.

In conclusion, it has to be observed that the caution shown by EFSA is justified by the necessity of paving the way before the introduction of these approaches for its action. This seems consistent with the premise that we are facing a progressive (yet, incomplete) de-materialisation of food safety risk assessment. However, we can observe a general trend towards the automation of food data collection and more proximity to the data source, especially in the case of IoT and smartphone-assisted food consumption data collection.

As the next section will show, while food safety risk assessment is still not pervaded by advanced data collection techniques and relies on observed data recorded in digital formats, a consolidated trend regards the use of machine learning to analyse data, predict and classify risk scenarios.

2.3 Machine learning techniques and food safety risk assessment

This section aims to briefly introduce and discuss advancements in the sector of machine learning applied to food safety. As the previous one, this section is meant to be inherently descriptive. Its relevance is due to some ethical concerns that these techniques originate in the course of their adoption. For the purposes of this section, it is necessary to approach food safety risk assessment in a more holistic way, in particular by enlarging the plethora of actors involved in the evaluation. We have seen that EFSA gathers data from different actors and makes effort to standardise incoming data. Keeping in mind that EFSA has no laboratories, data analysis can be performed either by EFSA itself on third parties' data (for instance, in reviewing the literature) or by third parties when gathering data to be submitted to EFSA. Such external actors might include Member States national authorities, independent laboratories working on behalf of business operators, the industry itself, and academic researchers. They produce both raw data and scientific works in forms of academic literature as outputs of their activity.

For the purposes of this section, we will therefore broaden the perspective of risk assessment and we will make a distinction between "data" and "literature". Their lines, however, should be blurred: scientific literature is often treated as data when Neural Language Processing (NLP) techniques are deployed and data are often attached to scientific works, thus becoming part of the literature (Tao et al., 2020).

2.3.1 Automation of literature reviews

In 2018, EFSA's commissioned study "Machine learning techniques for the automation of literature reviews and systematic reviews in EFSA" (Jaspers et al., 2018) is one of its first attempt to conduct an automatic reviewing of the scientific literature on a given topic[61]. As we have seen in §1.2.1, EFSA's Working Group experts have to rely on data and scientific literature to perform all the substantial steps of the risk assessment. Hence, the need of a tool capable of keeping track of scientific advancements by selecting relevant papers, extracting data, and ultimately reducing the workload of the reviewer. Authors concluded that "there is definitely an opportunity to use the introduced machine learning techniques for automating the screening of abstracts and full texts steps, at least partially" (Jaspers et al., 2018, p. 66).

The selected approach consists of machine learning techniques, mainly intended to automate both the abstract review and the full-text screening of scientific works. The task is approached as a classification problem in which the algorithm states whether the paper is relevant or not. This is decided according to a threshold probability of being relevant fixed at 0.5. Classifiers have been deployed using supervised, unsupervised and semisupervised methods. Classifiers were constructed using support vector machines, gradient boosting machines, neural networks, random forests, and ensemble methods. Multiple R software packages were used in the experiment.

Three case studies - the Isoflavones, used for dietary supplements, whose carcinogenicity has been under investigation (Food Additives and Food (ANS), 2015), the Qualified Presumption of Safety assessment (QPS) for additives, enzymes and plant protection products, the Emerging Risk Identification Support System (ERIS) - have been conducted. The results were encouraging, even though a limited amount of training data had been noted (Jaspers et al., 2018, p. 65) Overall, ensemble methods

[61] An other project, named "Testing a text mining tool for emerging risk identification" (Lucas Luijckx et al., 2016), based on a previous study (Marvin, Kleter, et al., 2009), was meant to support string-matching information retrieval of scientific literature with an ontology. The goal was to identify emerging hazards in the food chain by scrutinising the scientific literature focused on emerging trends. Despite not using machine learning techniques, it is noteworthy as a benchmark case study. While the original study relied on data retrieved from the Internet (e.g. news) alongside scientific journals, EFSA's tool cautiously limited its investigation to scientific papers

performed better than individual classifiers. The study also produced an R[62] tool capable of supporting the screening step of the literature review by offering in-context word-searching tools and instruments to extract data elements (Jaspers et al., 2018, p. 65).

Moreover, the project has delivered a R tool (EFSA, 2018c) for the automation of systematic reviews. A labelled CSV or TXT file is used as input. Then, the software lets the user free to choose among a wide range of options, including the input space (term-document matrix (TDM)[63], term-frequency/inverse-document frequency matrix (TF-IDF)[64], bi-grams or tri-grams[65] and topics according to Latent Dirichlet Allocation[66]), the size of the training set and the classifiers. Finally, an ensemble can be produced from single classifiers and saved to be used with new input data. The output consists of a CSV file displaying the classification ("relevant" vs "non-relevant") and operational data (accuracy, sensitivity, precision, recall, F1 score).

EFSA's approach to the automation of literature reviews is consistent with research trends outside the Authority identified by extensive reviews (Tao et al., 2020).

2.3.2 EFSA's "probabilistic turn"

Moving on now to consider probabilistic models used to predict emerging or possible hazards, this section presents an overview of some machine learning techniques that have been increasingly observed and studied by EFSA for the assessment of hazards. We will refer to this emerging trend as a "probabilistic turn" to highlight the non-deterministic nature of the results generated via these methods.

EFSA uses a wide range of tools to perform risk assessment. For instance, the Pesticide Residue Intake Model (PRIMo) model for pesticide chronic and acute exposure assessment (EFSA, 2018e) is based on equations grounded on scientific evidence. The model uses food consumption data, while calculation is performed

[62] R is a language and environment for statistical computing and graphics. https://www.r-project.org/about.html

[63] TDM is a large matrix displaying the frequency of each term in a corpus. Each row corresponds to a term, while each column represents a document. Rows and columns can be switched to originate a document-term matrix (DTM)

[64] TF-IDF is a frequency indicator based on the assumption that words highly frequent in one document while absent in other files will likely be relevant to the document under scrutiny

[65] Term document matrix using combinations of two, respectively three, consecutive words.

[66] Latent Dirichlet Allocation is a non-semantic detection system for word co-occurrence that allows to cluster documents according to the probability that their terms will appear with other terms related to the same topic (e.g. "tyre", "wheel", "clutch" are related to "car")

by an Excel file freely available on EFSA website[67]. In this evaluation, no machine learning technique is used.

Alongside simple spreadsheets like PRIMo, EFSA has also commissioned studies to evaluate probabilistic approaches to risk assessment. While a relevant part of its research already aims to forecast future trends, the novelty of this approach consists in the adoption of probabilistic analytical methods. It is crucial to point out the differences between "traditional" modelling and emerging "machine learning" approaches. In both cases, the output of the calculation consists of a likelihood. While traditional models, given the same initial conditions, generate the same output, machine learning models do not share this property and embed some elements of stochasticity in the final model[68]. Following Russell and Norwig's definitions (S. Russell and Norvig, 2010, p.43), we will refer to the traditional statistical modelling as "deterministic", whereas the machine learning approaches will be broadly identified as "stochastic" or "probabilistic".

For instance, a recently developed methodology regarding chemical contaminants exposure assessment relies on Monte Carlo simulation (AGES et al., 2019). This methodology makes use of random numbers to perform a given set of simulations in which exposures are calculated on the basis of observations of contaminated foods and food consumption data. The same attempt has been made with cumulative dietary exposure assessment of pesticides (Klaveren et al., 2019) and, when compared to the "SAS" software (EFSA, Dujardin, et al., 2019), encouraging results on the reliability of probabilistic models have emerged: authors observed that "Comparison of the results revealed that both tools produced nearly identical results and any observed differences are mainly attributed to the random effect of probabilistic modelling" (EFSA, Dujardin, et al., 2019, p.32).

EFSA's "probabilistic turn" is even more evident in the commissioned report "Machine Learning Techniques applied in risk assessment related to food safety" (IZSTO et al., 2017), which proposes both an extensive literature review and a decision tree for adopting machine learning techniques *vìs-a-vìs* deterministic models in the course of risk assessment. Following the literature review and the selection of machine learning techniques that could be deployed by EFSA, two different analyses have been performed, namely a) a comparison between deterministic and probabilistic approaches, and b) five cases studies in which stochastic methods have been deployed. Tables in the Appendix summarise their outcomes. First, two tables display the area of interest, the goal of the study, input data, the output (usually, a statistical model) and the algorithms that have been tested. Then, the third table

[67] `https://www.efsa.europa.eu/en/applications/pesticides/tools`

[68] This is a vital feature of machine learning models that characterise their advantages over traditional approaches. Stochasticity allows a high degree of accuracy towards new data by refining the model over time when new training data are added

classifies the algorithms on the bases of findings reported in the study[69].

2.3.3 Other studies on data-driven risk assessment

EFSA's attempts towards the adoption of machine learning techniques are not isolated. For instance, the use of probabilistic models for exposure assessment was theorised already in early 2000s', but the absence of well-defined collection methodologies was seen as an obstacle (Lambe, 2002)[70]. Today, the availability of Big Data and sufficient computational power makes possible the adoption of these techniques also by academic researchers, as this section discuss from prominent examples.

A study (Gu et al., 2015) has proposed a comparison between logistic regression and random forest to analyse causal relationships between the exposure to certain risks (i.e. direct contact with animals, consumption of raw/uncooked meat) and illnesses, even in case of missing values or high number of possible exposures. Random forest algorithms were proved to be more effective than logistic regression. Similarly, a short research (Ortiz-Pelaez and Pfeiffer, 2008) has shown the efficacy of combining of on-farm (animal movement) and environmental variables to generate a classification tree (C4.5 algorithm) capable of describing factors for risk profiles in cattle herds.

Pesticide residue monitoring can benefit from machine learning[71]. The combination of electric biosensors and Artificial Neural Networks (ANNs) has reached a sufficient degree of accuracy in screening different kinds of residue in pesticide monitoring (Ferentinos et al., 2013). If scalable, this system might increase the number of tests carried out in monitoring programmes.

An American study on environmental factors impacting vegetables and fruit (Strawn

[69] This final table aggregates algorithms fallen under the scrutiny of EFSA with a complexity and transparency/explainability score attributed by the authors of the report (see Tables 76, 77, 78). Transparency has been defined as "explanation ability/transparency of knowledge/classifications"(IZSTO et al., 2017, p.172) In its remit, our table has a descriptive purpose and should not be meant to endorse this evaluation or its definitions)

[70] This article is significant for its historical relevance, rather than its effective contribution to our discussion. Other issues, such as the availability of data and the computational resources needed for the deployment of machine learning techniques were not fully addressed

[71] In compliance with Regulation (EC) No 396/2005 of the European Parliament and of the Council of 23 February 2005 on maximum residue levels of pesticides in or on food and feed of plant and animal origin and amending Council Directive 91/414/EEC [2005] OJ L 70/1 and implementing regulations (e.g. Commission Implementing Regulation (EU) 2017/660) Member States are obliged to develop country-wide pesticide monitoring programmes to ensure that rules concerning maximum residue levels are respected

et al., 2013) is particularly significant due to the variety of data and machine learning techniques deployed. Authors included data on observed samples, topographical and spatial data to automatically generate a classification tree helpful to predict the presence/absence of food-borne pathogens linked to mereological or topographical conditions. Image recognition can be combined with digital microscopy or a faster and less expensive detection of parasites. For instance, this has been the case of *Eimeria* detection in domestic chicks using Bayesian classifier (Castañón et al., 2007). Support Vector Machine and Artificial Neural Networks have been used to recognise and classify species of harmful beetles (Bisgin et al., 2018).

Food consumption data represent a major source of information for risk assessment. Attempts have been made to lessen the burden of surveyed consumers while reducing the number of self-reported foods needed to infer compliance with dietary recommendations trough a decision tree classification algorithm. A study showed that age, sex and consumption data about 113 foods on the 3911 available in the UK National Diet and Nutrition Survey (3%) are needed to predict compliance with food guidelines (Giabbanelli and Adams, 2016) with 72–83 % accuracy depending on the food category. A similar study (Rosso and Giabbanelli, 2018) managed to increase the accuracy of 2.5% on average by including nationality and marital status and reducing the number of foods. Despite not being related to risk assessment, the inclusion of socio-demographic characteristics regarding parents and guardians has been required to perform a study on child consumption of foods and obesity, alongside children's physical activity data (Lazarou et al., 2012). In the fields of food consumption data analysis, dietary patterns are a consolidated trend (Hu, 2002). Clustering and Principal Component Analysis (PCA) has been used to generalise food consumption for pattern identification (Hearty and Gibney, 2013). Results have then been processed through Reduced Rank Regression (RRR) algorithms to correlate patterns and blood samples with diabetes (Batis et al., 2016). Similarly, nutrition patterns have also been proven to be successful co-predictors cardiovascular risk prediction (Rigdon and Basu, 2019).

2.4 The three informational components of risk assessment

To conclude this Chapter, it is necessary to analyse the key findings of this technical review under a more holistic perspective to support the legal and ethical discussions concerning the relevance of Big Data and their analysis in the domain at stake.

It has been preliminarily observed that food safety risk assessment activities - within EFSA or independent entities that maintain direct or indirect information flows with the Authority - are more datafied than in the past. To better understand the ongoing transformation process, it might be relevant to understand risk assessment in terms of *informational components*. In broad terms, an informational component is a segment of the more complex Big Data ecosystem that presents peculiar traits according to a given LoA. In the analysis that follows, the observable is the *origin* of the information at stake to be intended as the object of the datafication. Following our diaphoric conceptualisation of data presented in §1.2.1, the origin of the information consists of the object that an human or man-made agent takes as input to perform a given task which implies "datafication" activities. Such origin (e.g. some individual behaviour) can then be grouped (e.g. the behaviours of multiple individuals) and labelled (e.g."the human component").

In the following sections, informational components will be then identified and classified according to their origin, i.e. whether they have been recorded by analysing the behaviour of human beings, from other phenomena not directly related to individuals, or result from computations that take into account data as their input to draw conclusions that support decision-making processes.

2.4.1 The human component: food consumption data and background information

As noted, food consumption data are necessary to make predictions regarding the likelihood of future risks and their impact on individuals (§1.2.1). This information-type presents some noteworthy traits that should be mentioned for the purposes of carrying out a legal and ethical analysis in the next Chapters. To bridge the gap with following parts of this thesis a more holistic approach will be adopted to discuss the implications of the processing of this information, both from a technical and legal perspective.

When interviewed by external reviewers[72], EFSA's stakeholders suggested further improvements in the area of food consumption data collection: the Commission asked for more detailed data or consumption patterns; one national risk assessment authority suggested to link dietary intake to health data *by default*, to harmonise databases and to have at its disposal more group-specific data; the food industry called for more consideration of diet data at individual level and less relevance to adverse effects that are not justified by a real biological risk (p.70)[73].

[72] Ernst & Young External Evaluation of EFSA, Final Report 2012 https://www.efsa.europa.eu/sites/default/files/efsa_rep/blobserver_assets/efsafinalreport.pdf

[73] Interestingly, these suggestions came from answers to a segment of a questionnaire that was related to data quality, thus confirming the statement made in §2.2.3 that data availability and standardisation are a shared exigence among all the stakeholders

While the implications of the processing of background information (age, sex, marital status, region, rural/urban area, size of the household, household income, employment status)(Table 6.4 in the Appendix reports the complete list of personal data collected by national authorities and transmitted to EFSA in harmonised forms) are widely covered by the literature on privacy and data protection, studies on the processing of food consumption data and dietary patterns have been focusing on their proximity to the disclosure of health data. For instance, the discussion on *quasi*-sensitive data (Malgieri and Comandé, 2017) and the context of mobile health (Article 29 Working Party, 2015) have occasionally included data that are placed in-between legal classes of "regular" personal data and special categories of data. However, despite the relevance of mobile health apps and the likelihood of health data discovery by processing, our domain is far more intricate than a smartphone-mediated data gathering methodology that might reveal sensitive attributes.

Rather than focusing on the legal classification of the data at stake or on specific case studies, a more comprehensive analysis of food consumption data might be of relevance here[74]. This approach is split in two sets of observations: first, a "static" viewpoint discussed hereinafter highlights important findings on the connection between dietary information and personal and social identity; then, a "dynamic" perspective discussed in §2.4.3 identifies some noteworthy types of inferences that are technically feasible by processing food consumption data by automated means.

Let us first reflect on the connection between food and personal identity. While we need food to survive and we incorporate (from the Latin *incorporare*, derived from *corpus* (body) and the prefix *in-*) it through our mouth, eating is not associated solely with our survival instinct. As already noted, "diets cannot be reduced to their sole nutrition function" (Alemanno and Gabbi, 2016, p.151)[75]. Food preferences, whether be they entirely subjective or related to other physical conditions (allergies, intolerances, etc.), contribute to make each person an unique individual. Studies in neuropsychology suggests that children progressively align their food preferences to adults only by growing and developing a more complete body (Rozin et al., 1986). Moreover, let us think to Brillat-Savarin's most famous quote "Tell me what you eat, and I will tell you what you are" (Brillat-Savarin, 1841) or Feuerbach's: "Man is what he eats" (Cherno, 1963). Though in broad terms, these examples show some degree of connection between food preferences and personal identity.

The relationship between what we eat and our identity is also true as regards the

[74] Differently from cited papers, our findings should be limited to the domain of dietary intake information. Hence, our conclusions should not be generalised to all the *quasi*-sensitive data such as information regarding the number of daily footsteps or heartbeat rate of an individual

[75] As noted by the Authors, EFSA itself (EFSA Panel on Dietetic Products and (NDA), 2010) has justified the inclusion of food consumption data and background information for this reason when building profiles and dietary recommendations

belonging to certain social groups. For instance, we occasionally refer to other groups and people using the suffix *-eaters* or expressions such as "Frogs" for French, "Krauts" for Germans, "Macaronis" for Italians (Fischler, 1988). The same holds true for particular cuisines when they are associated to certain nationalities (like the Italian or the French one) in a manner that makes the cuisine peculiar to a national cultural heritage. The adherence to a particular diet - like veganism - can express one's belonging to a cultural movement (Cherry, 2006) or a philosophical belief[76] rather than simple food tastes. Religions make a wide use of food-related prescriptions (including fasting) to reinforce the belief: Catholic Canon Law prescribes the abstinence from meat every Friday, Ash Wednesday and Good Friday for everyone between 14 and 60 years of age; during the month of Ramadan in the Islamic calendar, fasting is recommended from dawn to sunset (daylight hours); in the Kashrut dietary laws, consuming animals listed in the 613 commandments is strictly prohibited. Despite the paucity of studies on this topic, political opinions are assumed to play a role in determining food preferences. Inferences drawn from alcohol consumption proved association between beer and spirits drinking habits and liberal ideology, holding economic, demographics and geographic differences constant (Yakovlev and Guessford, 2013). In a different study, it has been proposed that "left-wing" food habits are sensitive towards environmentalism, organic food and *farm-to-table* markets, whereas the "right-wing" ones tend to prefer frozen food, massive portions and energy drinks (Sasahara, 2018). Research has also focused on predicting overweight and diabetes (plus, incidentally, political opinions) rates from a large corpus of Tweets containing food-related hashtags (Fried et al., 2014).

In conclusion, consistently with our definition of "data", it could argued that the gathering of raw food consumption information entails the observation and the recording of characteristic traits of individuals and groups that regard their personal identity. However, preliminarily to the detailed legal analysis carried out in §3.4.3, it has to be observed that two different legal regimes apply: while individual food consumption data (i.e. those referred to an identified or identifiable person) are considered personal data for the purposes of data protection law (Alemanno and Gabbi, 2016, p.32), aggregated data (i.e. those referring to groups in which individuals are not or no longer identifiable) do not follow within the same category. Nonetheless, this substantial difference does not alter the relationship between food consumption and personal identity, being it individual or related to groups. The paradigm

[76] Case Casamitjana v The League Against Cruel Sports [2020] UKET 3331129/2018. A British employment tribunal found out that veganism meets the five criteria to qualify as a philosophical convictions: 1) It must be genuinely held; 2) It must be a belief and not an opinion or view point based on the present state of information available; 3) It must be a belief as to a weighty and substantial aspect of human life and behaviour; 4) It must attain a certain level of cogency, seriousness, cohesion and importance; and 5) It must be worthy of respect in a democratic society, not incompatible with human dignity and not conflict with the fundamental rights of others.

shift is only confined to the applicable law, whereas the general implications of the data processing at stake are left untouched. Notwithstanding the partial misuse of this wording from a legal viewpoint, this thesis will use "personal data" in an anti-formalistic meaning to define "data about person(s)", rather than adhering to the legal definition given by data protection regulations which require identifiability of the data subject to trigger the applicability of their provisions. The benefits of this operation will become clearer in the next Chapters.

2.4.2 The non-personal component: laboratory and experimental data

The definition of non-personal information can be deduced by the Free Flow of Non-Personal Data Regulation[77]. Art. 3 states that non-personal data consists of data other than those mentioned in Art. 4(1) of the GDPR, i.e. information related to an identified or identifiable person. This implies that anonymised or aggregated information fall within this regime, unless individuals are made identifiable through de-anonymisation techniques (single out) or by unique traits make clear the linkage between an individual and her or his data[78]. Despite such clear line between personal and non-personal information, we will refer to "non-personal component" as data which have not been collected, observed or recorded from human sources, or following the working definition given above, "data that are not about person(s)".

As we have seen, non-personal data represent the complementary information needed to perform risk assessment. While the public availability of these datasets should be recommended to perform an independent cross-validation of the studies, this is not the case in reality, especially when the commercialisation of products generate strong business interests. Let us considering the following example: in 2015, the International Agency for Research on Cancer (IARC) published a monograph about the carcinogenicity of the pesticide active substance glyphosate and claimed that chemical had met the criteria for classification as a "probable human carcinogen" (Fritschi et al., 2015). In the same year, EFSA replied to the Renewal Assessment Report (RAR)[79] request made by the German Federal Institute for Risk Assessment

[77] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union [2019] OJ L 303/59

[78] Article 29 Working Party Opinion 05/2014 on Anonymisation Techniques, available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[79] The RAR is a mandatory requirement for the continuation of the authorisation regime for pesticides. It has to be submitted to a competent national authority and, in turn, to EFSA by the applicant of the renewal procedure.

(Bundesinstitut für Risikobewertung, BfR) for glyphosate and concluded that the chemical had an unlikely carcinogenicity potential (EFSA, 2015a).

Members of the European Parliament were denied to have access to confidential data, while some researchers claimed the existence of omissions (i.e. missing data) on the evidence submitted to the BfR (Portier, 2015). As a reply, EFSA confirmed the adherence to standard protocols for data analysis and, therefore, the quality and the transparency of its review (EFSA, 2015c). Following the letter, Portier and colleague argued that "to maintain transparency, IARC reviews only publicly available data. The use of confidential data submitted to the BfR makes it impossible for any scientist not associated with BfR to review this conclusion" (Portier et al., 2016).

When non-personal information is shared among the industry, independent laboratories, competent authorities at EU or Member States level, data quality has to be guaranteed. Since EFSA might not have sufficient resources to perform independent studies and its *ex novo* data generation is limited (EFSA, 2015b, p.8), missing or altered third-party data represent a concern. At it will be argued in the following sections, this issue might be amplified by the use of machine learning techniques that tend to replicate existing patterns to predict future trends.

Let us consider the "Monsanto Paper" scandal (The Guardian, 2017). Dozens of pages of EFSA 2015 Renewal Assessment Report on Glyphosate were alleged to be copied by scientific papers "ghostwritten" by Monsanto, a worldwide market leader in this segment (McHenry, 2018). Seemingly, PAN Europe NGO has raised doubts concerning the practices of a laboratory in Hamburg, alleged to "distorting the data to please its clients" (PAN Europe, 2020). Collected data were also included in dossiers submitted in the course of the evaluation procedure of pesticides and RAR[80].

In these two scenarios, missing or altered data seem of particular concern since the possible mistakes in data collection might be replicated in further studies relying on such biased literature, in particular when machine learning techniques are deployed. The amount of the risks linked to poor data quality escalates due to the increasing quantity of data and sources highlighted in the previous sections.

Notwithstanding EFSA's efforts made towards standardisation to make data widely accessible and interoperable, two major issues persist: on the one hand, the protection of confidential information limits the public availability of data; on the other hand, poor data quality might be a concrete obstacle to the trust in food safety system due to scandals linked to wrongful data collection. Chapter 3 will examine the legal response to these issues.

[80] At the time of writing, formal investigations are still running

2.4.3 The machine-generated component: derived and inferred data

So far, this section has discussed two stand-alone informational components of food safety risk assessment. This subsection will focus on their interplay and on the possibilities given by analysing the combination of personal and non-personal information to gather evidence useful for risk assessment purposes. In this section, we will refer to the machine-generated component as those information that originate from data analysis rather than observed from tangible phenomena. Differently from "raw" data, this information is integrated into evidence[81] and decisions are taken on top of these outputs[82].

First, findings emerging from the technical review and the case studies performed by EFSA highlight promising results. This is line with EFSA's expectations and strategies for the future, thus making the adoption of these techniques foreseeable in the upcoming years. Alongside more precise results and more efficient procedures to which the Authority has devoted attention (Cappè et al., 2019), discussion on some emerging concerns is needed.

In particular, data fallacies which consist of mistakes in data collection, analysis or interpretation, represent a major challenge for the ongoing datafication process. These kinds of errors can be classified according to three categories:

- Data-driven fallacies. For instance, a wrongful construction of training sets for machine learning algorithms might originate sampling biases, incompleteness due to selection criteria ("survivorship bias"), or manipulation of data grouping criteria ("gerrymandering").

- Analysis-driven fallacies. Underfitting and overfitting of statistical models is a well-known issue of machine learning modelling that pertains to the under- or over-representativeness of the statical model in relation to the training data. When underfitting, the model lacks of a sufficient descriptive power to identify a generalisable pattern. Overfitting, instead, consists of the poor generalisability of the model due to its extreme adherence to the training data. "Regression towards the mean" mistake occur when phenomena are generalised

[81] Our focus will be limited to the processes of data analysis, combination and integration finalised to generate evidence as intended by EFSA (EFSA, 2015b). The "leap" from data to evidence also concerns epistemological and methodological questions. However, we will confine the remit of our study to what pertains to EFSA risk assessment activities

[82] In the distribution of competences pertaining to risk analysis, only risk managers are in charge of taking decisions. Despite the high persuasiveness of its opinions, EFSA, i.e. the risk assessor, shall be placed outside the decision-making process (§3.4.3 - Accountability and Redress)

using statistical mean in order to prevent peaks or unexpected results.

- Interpretation-driven fallacies. "False causality" is a wrong assumption of cause-effect relationship for trends that simply present spurious similarities; relying on summary metrics might hamper the significance of differences in raw data; "cherry picking" (or confirmation bias) is the practice of selecting results that fit certain claims while excluding others; finally, the so-called "Gambler's fallacy" is the trend to believe that something unusual according to the data will not happen in the future (or vice versa)

Let us discuss some significant examples by means of a theoretical experimental framework. In the following figure, five stages are displayed. First some data constitute the training set of one (ore more) supervised machine learning algorithm used to obtain results. Its outputs are transposed in a scientific paper similar to the ones mentioned in our technical review, thus framed as classification problem (relevant / non-relevant). Then a final user - let us say, a risk assessor - retrieves the paper by means of a machine learning algorithm that performs an automated literature review as the one described in §2.3.1. Scientific papers, in the last stages, constitute training sets for the algorithms which perform the literature review.

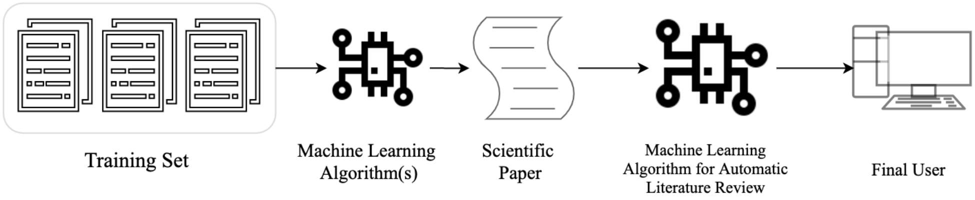

Training Set
Machine Learning Algorithm(s)
Scientific Paper
Machine Learning Algorithm for Automatic Literature Review
Final User

Figure 2.4: Automation of Literature Review

The reality is, of course, far more complex that scenario displayed above. In fact, the data-chain described so far might include several agents that make use of machine learning techniques. This hypothetical setting is likely to raise concerns regarding the propagation of inherent model biases that could be propagated to other studies and reach the "evidence" level in EFSA opinion. The pictures below show some noteworthy cases of biases.

Fig. 2.5 below shows three non-biased data-chains (A, B, D). In these chains, colours in the training sets represent some degree of diverse input data (e.g. food consumption data belonging to diverse ethnic groups). Instead, chain C does not presents the same amount of diversity *within* itself. This situation might emerge as a consequence of the aforementioned data-driven fallacies. Line C algorithm generates results that are transposed into a biased paper: despite being correct from a mathematical perspective, its results might be fallacious if we take into account that certain food patterns are under-represented. Paper C propagates the bias to the final user by being embedded in the model generated by the machine learning algorithm that performs the automatic reviews. This situation will be referred to as Type A bias.

This scenario could also occur in the absence of machine learning models deployed across the data-chain. However, their presence considerably increases the risks associated to Type A bias as some of the models used in the scenario might not allow an in-depth scrutiny of their functioning ("black-box" problem, discussed at §4.1.2) or if training data are not made available to the final user and her or him can only trust the overall results (e.g. precision and recall).

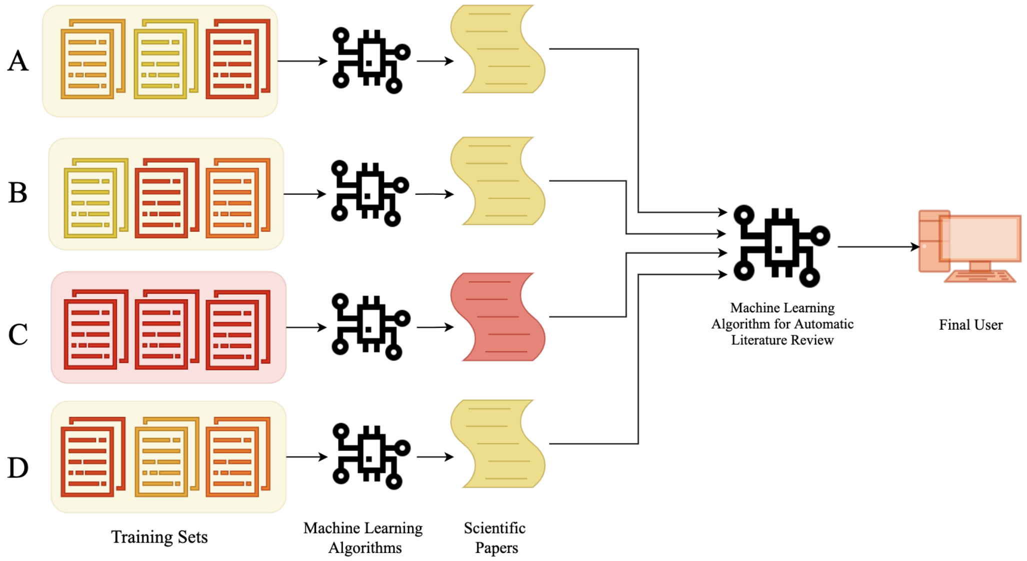

A
B
C
D
Machine Learning Algorithm for Automatic Literature Review
Final User
Training Sets
Machine Learning Algorithms
Scientific Papers

Figure 2.5: Bias Propagation - Type A Bias

One might thing that the problem of Type A bias propagation could be solved by adding some degree of diversity *within* paper C,. Fig. 2.6 shows that, in reality, another kind of bias might emerge, for instance if selected papers come from the same author. This is the case of absence of diversity *among* rather than *within* papers that are automatically scrutinised. This scenario will be named after Type

B bias. Its consequences are the lack of diversity in candidate papers selected for literature review and fallacies in the results presented to the final users since only one perspective is offered despite diversity in the training sets.

Since Type B bias emerges from the literature, it may be qualified as a distributed form of the so-called "confirmation bias". While this scenario might occur without machine learning deployment, it can be reinforced by the use of such probabilistic approaches. For instance, if the scientific literature agrees on the safety of pesticide *X*, than the algorithm will likely assign more relevance to papers confirming such agreement. Moreover, this implies that alleged 'ghostwriting' cases or other scandals will be harder to detect if there is not sufficient oversight over weights and relevance scores assigned by the algorithms.

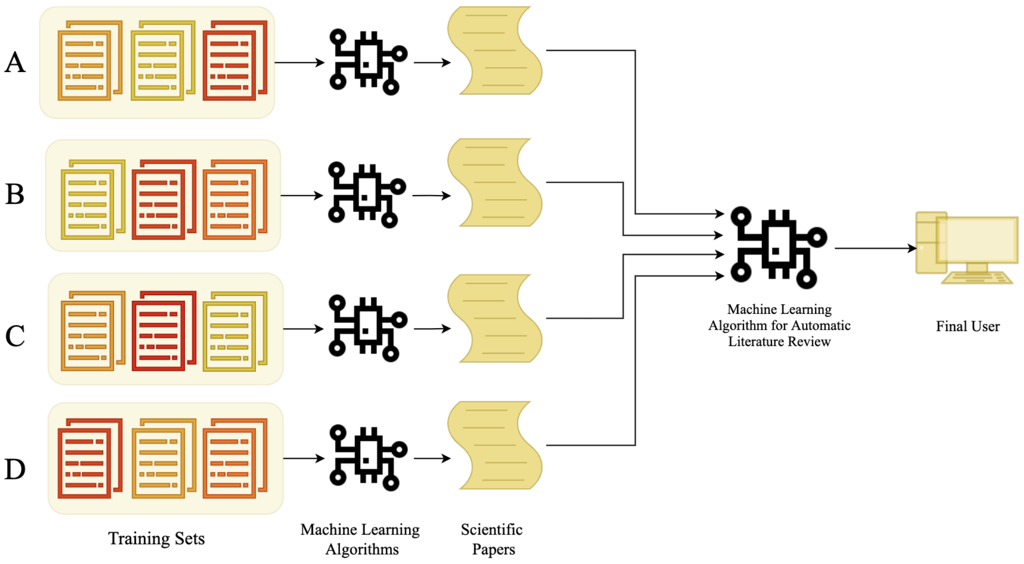

A
B
C
D
Training Sets
Machine Learning Algorithms
Scientific Papers
Machine Learning Algorithm for Automatic Literature Review
Final User

Figure 2.6: Bias Propagation - Type B Bias

Crucially, adding diversity *among* candidate papers solves Type B bias but might be insufficient in ensuring that Type A bias is not propagated from training sets to the final users. Figure 2.7 below shows this scenario: while data-chain C has Type A bias, non-biased papers seem to mitigate the bias by displaying non-biased results to the final user. However, more relevance might be attributed to paper C due to the internal setting of the automated review algorithms as its biased results might display higher accuracy in comparison to papers in chains A, B and D. When this is the case, Type A bias might still cause fallacious results. Therefore, this scenario is still sub-optimal.

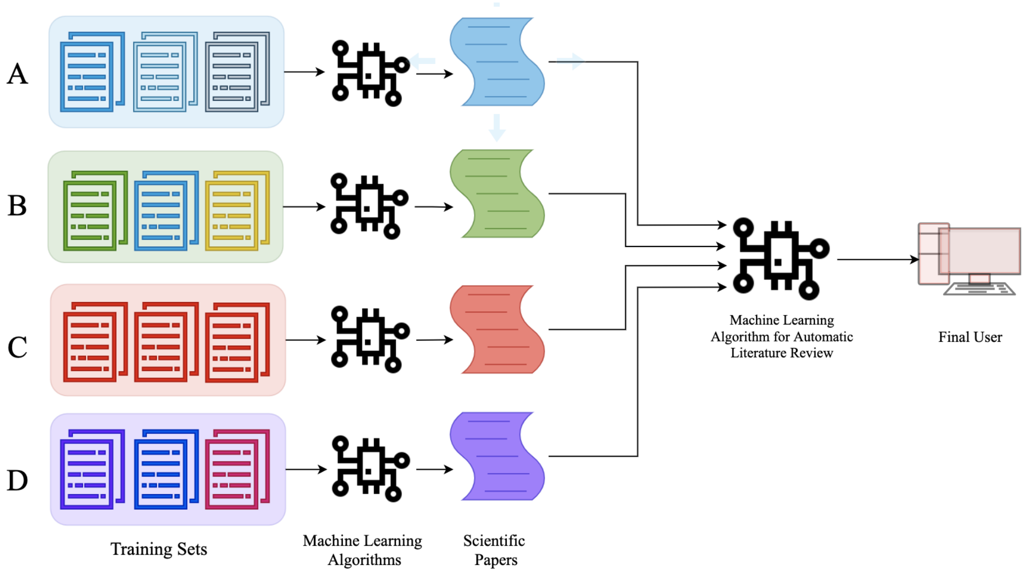

A
B
C
D
Training Sets
Machine Learning Algorithms
Scientific Papers
Machine Learning Algorithm for Automatic Literature Review
Final User

Figure 2.7: Bias Propagation - mitigated Type A Bias

Finally, the optimal situation can be the one displayed in Fig. 2.8 below. Diversity *within* and *among* papers guarantees that non-biased results are presented to the final user.

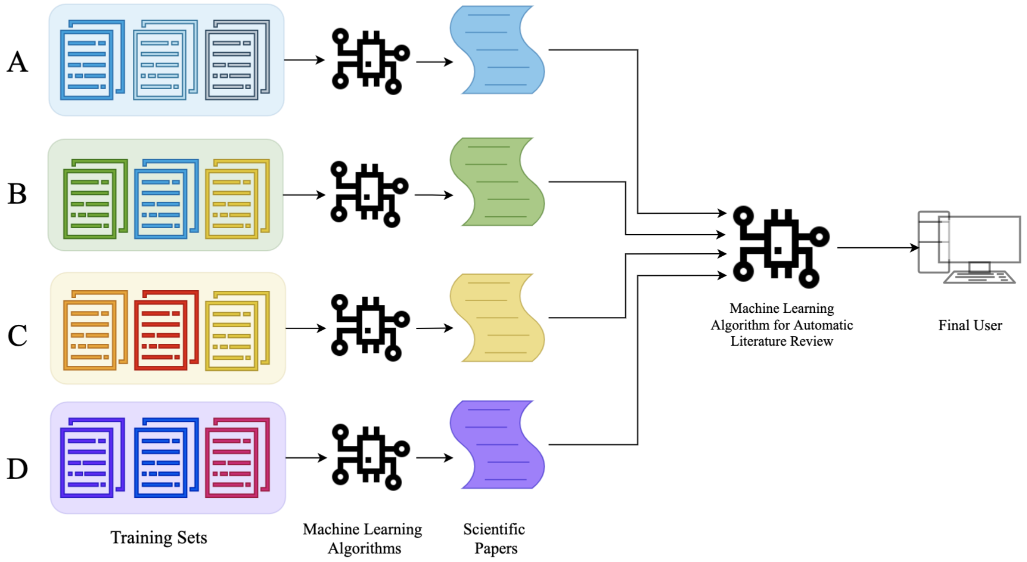

A
B
C
D
Training Sets
Machine Learning Algorithms
Scientific Papers
Machine Learning Algorithm for Automatic Literature Review
Final User

Figure 2.8: Bias Propagation - Absence of bias

Once clarified the phenomenon of bias propagation, let us examine some of its implications. One particular kind of bias that might originate from dietary information collected for risk assessment purposes. As mentioned above, they can be used to infer other personal information, namely religious and ethical/philosophical believes, political opinions or health status, all of which fall within the special category of personal data for which the GDPR call for stricter rules. When this is the case, Recital 75 of the GDPR points out that the data processing could generate "physical, material or non-material damages" which, in turn, affect the rights and freedoms of natural persons. In the scenario at stake, a direct damage for an individual caused by the processing of this information can occur only if his or her data is undergoing processing[83], whereas it is unlikely for individuals whose data is not analysed or if personal data are anonymised/aggregated to an extent that individual damage is very unlikely or virtually impossible. Nevertheless, when discussing Type A bias, we noticed that the hypothetical food safety risk assessment did not take into adequate account certain food pattern, especially those linked to a minoritarian group. Following the deployment of machine learning techniques, underestimation or overestimation of certain food patterns in input datasets (in particular, in supervised approaches) may thus lead to subtle forms of collective or group discrimination.

The question of bias is also linked to the shift from deterministic to probabilistic methods, which brings along concerns pertaining to the accountability of risk assessors. Deterministic algorithms are characterised by the an equality relationship such that, given the same input and a functioning software, the output will always be the same. Hence, the correctness of deterministic results can be assessed by analysing whether input data were correctly inserted in the system and the algorithm executed all the planned instructions according to the set of commends given by the programmer. Vice versa, probabilistic modelling is characterised by results that are expressed in terms of likelihood. As such, they always embed a statistical error (e.g. false positives/false negatives) due to their own nature. Differently from deterministic scenarios, such errors can occur despite the use of high quality input data and the correct functioning of the software. Since this factor might leave open the questions regarding how these sorts of mistakes and failures could be identified and who would accountable for them.

Finally, It is also worth mentioning that the possibility of combining personal and non-personal information is even more feasible in industry-led studies. The 2018 Bayer-Monsanto merger have created a *de facto* data conglomeration that makes possible the collection of experimental, agricultural and personal information, con-

[83] For instance, in the event of a data breach (Recital 85). To assess the magnitude of the risks, it is worth mentioning that EFSA food consumption database contains $\simeq$ 100.000 individual records that aim to generalise the behaviour of more than 500 million individuals

trol over scientific publications and resources to compute large quantities of data by deploying cutting-edge methodologies. While it is still not possible to ascertain the informational implications of this merger, its consequences might range from the competitive advantage offered by such extraordinary amount of information[84] to the possibility of commercialising high-quality data with high inferential capability.

2.5 Chapter Synopsis

In this section, relevant technical aspects describing the ongoing datafication of food safety risk assessment have been discussed. Understanding the technicalities of this transformation by analysing its informational components should allow for drawing general conclusions regarding how this shift might impact individuals, groups and the society, to identify key challenges and, eventually, to draft possible solutions.

The ongoing transformation becomes clear if we consider that the generation of evidence happens in de-materialised forms. From the moment in which human behaviours and other phenomena are recorded in digital forms, issues such as data quality, standardisation, interoperability, and so forth, come into play. Then, the automated analysis of this information raises further issues - including biases, error assessment - which massively differ from the previous ones for being completely detached from the informational source and partly unknown to the risk assessor.

The deployment of machine learning algorithms can also be seen as the insertion of a further step in the risk assessment chain. Food is a ’credence good’ (Lee, 2017)[85]. Humans and animals do not assess the safety of their foods in ways other than some intuitive (*naïve*) controls made using their senses and instinct (for instance, unexpected or bad smell sometimes suggests that food is not edible). The "hard tasks" of risk assessment - i.e. those that present a medium level of complexity - are delegated to institutional risk assessors which dispose of the capability and the instruments to perform the risk assessment. In turn, risk assessors delegate to machine learning algorithms the "harder tasks" that involve large, mutable and heterogeneous data, thus requiring higher-level computations. In this scenario, we confront with a *delegating delegation* situation represented by the image below.

[84] Big Data and competition are a key research topic under the scrutiny of national competition authorities since the notorious French/German report of 2016

[85] Consumers can observe the utility they derive from the credence goods only *ex post*. Instead, they cannot judge *ex ante* whether the type or quality of the good they have received is the needed one

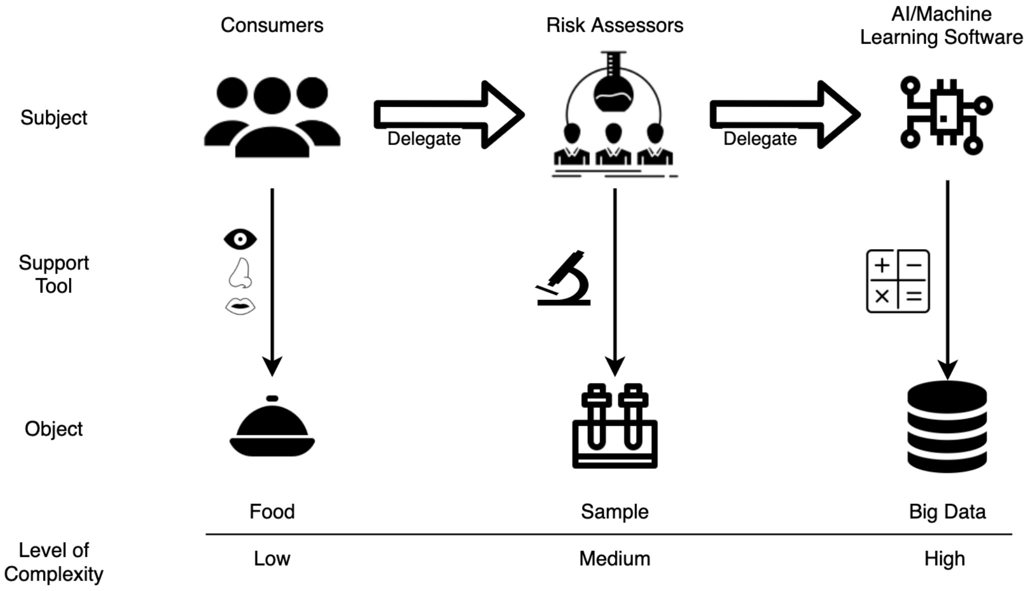


Figure 2.9: Delegating Delegation

Is the use of machine learning over Big Data similar to the use of a microscope for what concerns the relationship between the user and the tool? One could argue that there is no difference between these artefacts. Both can be conceived as mere tools that support the scientist in carrying out risk assessment. By relying on Floridi's interpretation of technological orders (Floridi, 2014, Ch.2)[86] while the microscope consists of a - yet advanced - first-order technology as it interacts with a tangible object and the machine recording data from the microscope (or otherwise interacting with it) is a second-order technology, machine learning algorithms exclusively processing data with little or no human intervention can be considered a third-order technology.

[86] Floridi's theory of technological orders consists of an ontological re-engineering of technologies. A triadic relationship between a *prompter*, an *user* and a *technology* is the fundamental premise: the prompter sends some kind of signals in the user, which reacts to them by using a technology. Let us consider first-order technologies, like the hat. The prompter (the sun), sends signals (light) to the user (human being), which reacts by protecting her or his head with a technology (the hat). First-order technologies place themselves between the nature and mankind. Second-order technologies, instead, are placed between human beings and other technologies: for instance, a screwdriver (second-order technology) allows men and women (users) to interact with a dishwasher (technology). When introducing third-order technologies in the pictures, human beings simply disappear. *Anything-to-anything* or *a2a* interactions are peculiar of third-order technologies, which are placed in-between technologies.

An other significant difference has to be noted as regards their degree of autonomy displayed by these tools (Fossa, 2018). On the one hand, a scientist outsources a portion of a task to the microscope aiming to make her or his duty (i.e. the observation of a phenomenon) feasible; on the other hand, outsourcing something to a machine learning system entails the delegation of the whole task to a tool capable of minimising the efforts needed to achieve trustor's (i.e. the risk assessor) intended goal (Taddeo, 2017). While the microscope *supports* the risk assessor in a task, the scientist *delegates* a whole Big Data-related task to a machine learning algorithm with a restricted human intervention that is limited to the *ex-ante* programming activities and the *ex-post* observations of the results.

Such form of delegation generates several element of risks, the first being linked to trust deriving from delegation, rather than supervision, made possible by the progressive (yet, still ongoing) refinement of machine learning system (Taddeo and Floridi, 2018).

Not only it is proven that the level of trust in the competent authorities is low[87], but it is likely that the use of incorrect input data and the deployment of machine learning techniques might further generate distrust on food safety authorities, a constant trend that occurs every time algorithms are proven to be unreliable (Fossa, 2019). In particular, this is true when these two factors are combined and scepticism towards their use is common in the scientific community. Trough its voice, distrust might be spread in the public opinion, ultimately bringing negative effects on the whole sector, including both the Authority and the market. An excessive faith on probabilistic results could be perceived as following the voice of an oracle, with little or no understanding over its logic (Mittelstadt, Allo, et al., 2016, p.4).

Trust in the algorithm is a crucial component of the aforementioned kind of delegation (Taddeo and Floridi, 2018). Overestimating the potentialities of machine learning and Big Data might generate excessive expectations towards probabilistic results. Striking a balance between responsiveness and certainty is also a massive challenge due to two clashing interests. While the industry calls for faster (and, possibly "smart") procedures, certainty of the results cannot be achieved without cautious scrutiny and extensive tests, which require more time to be performed.

As mentioned at the end of the previous subsection, the accountability for the use of machine learning softwares represents another source of concern. Alongside the

[87] EU Commission, 'Refit Evaluation of the General Food law (Regulation (EC) No 178/2002' SWD(2018) 38 final. The initiative has been launched as a reply to the citizens' legislative initiative "Ban Glyphosate and Protect People and the Environment from Toxic Pesticides" that followed the Monsanto Paper scandal. Taken together, these facts highlight the lack of trust on risk assessment activities and the scepticism towards the validity and independence of their results. More on this topic will be discussed in Chapter 3

risks related to the use of probabilistic models *vìs-à-vìs* deterministic algorithms as regards the assessment of failures, delegation entails some kind of allocation of the social risks linked to such failures. While the former question pertains to *how* such errors could be detected, the latter asks *who* should be responsible for the possible damage. Despite the higher degree of autonomy of machine learning softwares in comparison to other tools, their goals are always aligned to the one of the risk assessor (i.e. the delegator) (Bryson and Kime, 2011). Therefore, accountability mechanisms might have to be re-conceptualised to prevent immunities or ”grey areas” based on the assumption that machine learning softwares by-pass human agents and discharge their responsibility.

3

EU Food Law and Policy on Openness and Transparency of data

3.1 An overview of the food safety policy framework

Having discussed current and foreseeable Big Data analysis practices in food safety and some related concerns, this Chapter outlines the present and the future landscape of risk assessment from a legal point of view. As stated in §1.4, this is necessary to align our findings to the principles already in place in this regulatory framework. To do so, this Chapter presents a commentary on some recent normative attempts and interpretative analysis that have been made to solve data-related issues. In the Introduction, certain key aspects of the legislative framework - including the fundamental division of powers between tasks related to risk assessment, risk analysis and risk communication - were presented. It is now necessary to investigate them under a specific data-centric perspective[88]. For illustrative pur-

[88] Our analysis investigates several sets of provisions united by their data-centric focus. To select norms to be analysed we will only refer to provisions in which data are 'processed'. The GDPR (Art. 4(1)(2))) and the the Free Flow of Non-Personal Data Regulation (Art. 4(3)(2)) align their definition of 'processing' as any the operation or set of operations which is performed on data or on sets of data in electronic format, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction,

poses, an historical narrative - from the origins to the 2019 reform - will be adopted in **§3.1**. More emphasis, however, will be given to the latest amendments, i.e. the 2019 Transparency Regulation. Three sectoral regulations will be then discussed in detail **§3.2** due to the different solutions that have been adopted when dealing with critical market sectors in which conflicting interests related to the processing of Big Data tend to clash.

As it will be shown, the regulatory framework under scrutiny has to reconcile several different interests - including the functioning of the EU internal market, the protection of human health, the scientific excellence of the competent authorities - brought forward by many actors, namely the industry, EU citizens, independent scientists and EFSA. As noted earlier, data are crucial - though in different manners - for all these actors, hence the need of reconciling their concerns (e.g. the protection of commercial investments) when general interests (e.g. transparency of data) gain significance towards data-related matters. As it will be argued, regulators have mostly focused on issues pertaining to raw data governance rather than on their analysis, thus leaving space for formulating hypotheses on how to solve some unanswered concerns identified at the end of Chapter 2.

The jurisprudence of the Court of Justice of the European Union (CJEU) will also enrich the following discussion by providing insights into the meaning of the principles upon which the food regulatory system and its data-related provisions have been drafted. **§3.3** discusses this jurisprudence and academic comments. A broader perspective is then taken in the following **§3.4**, which discusses "neighbour" current issues - including data ownership and algorithmic transparency - alongside other foreseeable legal challenges. A Synopsis (**§3.5**) summarises the research areas covered by this Chapter and sets the discussion for the next one.

3.1.1 The origins: the 1997 Green Paper and the 2000 White Paper

The early development of the EU food safety legal framework is linked to food crises that affected Europe in the 1990s resulting in "food scares" (Knowles et al., 2007). Together with the aforementioned BSE/"mad-cow" disease, the Belgian Dioxin Affair[89] and cases of Foot-and-Mouth Disease raised concerns for their

erasure or destruction

[89] The 1999 Dioxin crisis affected Belgian feed manufactures and, in turn, to food producers in Belgium, France and the Netherlands. The inefficiencies of the food system became clear when a notification of an investigation carried out by an independent veterinarian, Dr. Destickere, was brought forward in March, while confirmation studies from the Belgian government took more than one month to be completed and measures taken by the government were in force only in May. Please

effects in human and animal welfare, including in their economic perspective[90].

The 1997 Green Paper[91] marks the beginning of the risk-based regulation of food safety in the European Community (Lee, 2017). Six goals were identified:

- to ensure a high level of protection of public health, safety and the consumer;
- to ensure the free movement of goods within the internal market;
- to ensure that the legislation is primarily based on scientific evidence and risk assessment;
- to ensure the competitiveness of European industry and enhance its export prospects;
- to place the primary responsibility for safe food on industry, producers and suppliers using hazard analysis and critical control points (HACCP) type systems, which have to be backed up by effective official control and enforcement;
- to ensure the legislation is coherent, rational and user-friendly.

The 1997 Green Paper shows a multi-faceted approach that aims to find a *one-fits-all* solution for the protection of consumers' health, the flourishing of the internal market through harmonisation and evidence-based risk assessment. Criticism emerged due to the complexity of such regulatory attempt (Vos, 2000). Part IV of the Green Paper is of particular interest for what concerns data and evidence governance. Specifically, it establishes that in case of scientific uncertainty or absence of data, the precautionary principle should apply.

This principle has been defined as the necessity that, "in cases of serious or irreversible threats to the health of humans or ecosystems, acknowledged scientific uncertainty should not be used as a reason to postpone preventive measures" (Jasanoff,

note that this reconstruction has been drafted according to the information provided by academic commentators (Lok and Powell, 2000) not subject to peer review

[90] For instance, EFSA (EFSA, 2006) noted that "Foot and Mouth disease (FMD) creates severe epidemics that reduce productivity and can profoundly affect the livelihoods of those rural communities that depend almost entirely on livestock agriculture. An important impact, often overlooked or disregarded, is the emotional impact on farmers, their families and their communities. The recent 2001 FMD outbreak in the UK led to an increase in suicides and human depression. This has been studied in the associated Dutch 2001 FMD outbreak when a marked increase in post-traumatic stress was observed"

[91] Commission of the European Communities, The General Principles of European Food Law - Commission Green Paper. COM (97) 176

2016, Ch.1, 2) (Martuzzi, Tickner, et al., 2004, p.7). The correlation between absence of data and measures to be taken explains the relationship between risk assessment and risk management. As long as the lack of data originates scientific uncertainty towards a potential threat, preventive measures have to be taken by risk managers. While this is enough to remark the centrality of data since the beginning of EU food legal framework, a direct equivalence of lack of data and scientific uncertainty has to be noted. In the Green Paper, there is no difference between the two concepts: scientific uncertainty is not a consequence of the absence of data and it could persist despite the availability of information regarding the threats. Moreover, since EU food legislation was meant to be a reply to food scares intended to restore faith among consumers regarding their health and the safety food industry, EU food regulators decided to adopt two specific goals, i.e. ensuring consumer protection and competitiveness of food-related market sectors. In 1997, evidence-based risk assessment and precautionary principle in risk management were referred to as instruments to catalyse the market towards these objectives. From a governance viewpoint, the Commission was empowered both of risk assessment and risk management competences. The Green Paper did not put emphasis on conflict management, especially over data, and on the independence of scientific assessment. The principle of transparency was mostly covering the clarity and easy identification of the legislation regulating risk analysis, once again to less the burden for market operators.

Before analysing the 2000 White Paper, it is worth mentioning that the 1997 "Medina Report"[92] released by the EU Parliament highlighted the inadequacy and the lack of resoluteness of the Commission Standing Veterinary Committee (appointed by Member States) and the Scientific Veterinary Committee (scientists) in evaluating BSE data independently, possibly due to the alleged political pressure under which risk assessors were put by the British Government (Para 2). A crucial aspect of the Medina Report is the fundamental role played by transparency. The very first recommendation of the enquiry is to promote "the widest possible dissemination of relevant research data and findings" as a transparency measure. Significantly, the principle of transparency was broaden beyond its original scope (i.e. the accessibility of food legislation) to include Committees' activity and research data.

Such renewed remit will be eventually confirmed in the aftermath of the Report. Taking into account the Medina Report, the 2000 White Paper[93] adopted a more proactive approach to the matter of data analysis. First, the White Paper highly recommended the establishment of an independent Authority in charge of performing risk assessment and monitoring. Second, its powers should have been con-

[92] Report on alleged contraventions or maladministration in the implementation of Community Law in relation to BSE, Part A.: I. Results of the Enquiry; II. Recommendations for the future; III. Minority Opinions (published separately) - Temporary Committee of Inquiry - A4-0020/1997

[93] Commission of the European Communities, "White Paper on Food Safety". COM (1999) 719

sistent with the new "Farm to Table" approach, which aimed to cover the whole food chains and multiple stakeholders, including consumers. Third, scientific advice should have been integrated with risk management and risk communication, three components that were clearly defined for the first time. Fourth, precautionary principle would eventually be confirmed as a crucial guidance, but limited to risk management.

In the absence of an already established independent food safety authority, the White Paper only broadly mentioned risk assessment data in Chapter 3 (Alemanno and Gabbi, 2016, Ch.1). The availability of accurate, up-to-date, scientific data is prioritised and only certain information-types (epidemiological information, prevalence figures and exposure data) were mentioned. A brief nod was also made to networked data collection methods.

Chapter 4 of the White Paper detailed the tasks and of the future Authority, which expectedly include information gathering and analysis. Independence, scientific excellence and transparency were pointed out as steering principles for which the Authority should be accountable. While "independence" and "excellence" regard personnel selection and appointment, "transparency" covered both the findings and the processes through which scientific outputs were reached, in particular when minoritarian scientific opinions were presented (Alemanno and Gabbi, 2016, p. 266). While a massive dissemination of the opinions was guaranteed by citizens' right to access to public documents and by the publication of these conclusions on the Internet, a general principle of "confidentiality" of scientific discussions was endorsed. Interestingly, this was the first mention of the clash of interests between commercial necessities of food business operators that might be harmed in scientific discussions within the Authority and openness for public scrutiny. However, since the White Paper constituted just a broad set of recommendations for policy-makers, detailed provisions on how to this balance of interests was to be addressed were not presented.

While transparency in risk assessment partly overlaps with risk communication as Chapter 7 set out, data dissemination was not covered. Instead, imperative implementations were set out as follows: the Authority must be guided by the best science, be independent of industrial and political interests, be open to rigorous public scrutiny, be scientifically authoritative and work closely with national scientific bodies.

An interesting provision was set out in Para 50: "[T]he Authority must be able to guarantee a real-time evaluation and response of the outcome of these programmes, ensuring that real or potential hazards are rapidly identified. In addition, the Authority will need to develop a predictive system that will allow the early identification of emerging hazards, so that crises can be avoided where possible". Likewise, the need of collecting food intake information into an *ad-hoc* database was mentioned in Para 74 in relation to the necessity of monitoring pesticides, residue limits and other contaminants.

In conclusion, these first steps of food safety legislation show a progressive detailing of a new approach towards evidence-based forms risk assessment. The final picture that we can draw from these first regulatory attempt is a methodology of grounding risk-managing measures upon scientific data. Layers of intermediation have been progressively introduced in the shift from the Green to the White Paper, in particular in the integration of data into evidence and, in turn, into scientific opinions. Technical implementations, including databases and predictive systems, were also proposed.

By acknowledging the political implications of food-related decisions, the independence of scientific assessment has led to the proposal of an authority placed outside the policy-making bodies and granted of separate tasks. The principle of transparency has followed a similar path. From its mere instrumentality to independence of the assessors, it has been progressively enlarged by the White Paper to include the so-called "reactive" and "proactive" approaches to the publication of documents (Faini and Palmirani, 2018) for reasons of public scrutiny and democracy. These approaches mark the beginning of the doctrinal conceptualisation of transparency in food law, which is grounded on public consultation and public information (Rusconi, 2016, p. 461). Both are intended to promote trust in food safety authorities. However, at the moment of drafting the White paper, data were placed outside the discussion and attention was only given to the disclosure of documents. While this seems in continuity with the Green Paper, this decision seems in contrast with the Medina Report, which had called for the "widest possible dissemination" of scientific data.

3.1.2 Fundamental traits of the General Food Law (Regulation 178/2002)

General scope of the GFLR: legal basis, goals and the precautionary principle

Today, the EU food safety legal framework consists of several sets of rules regulating diverse phenomena related to the food chain, from production to consumption and controls. This wide range of measures thus includes ingredient-related provisions (including rules on the use of additives, flavourings, enzymes) and consumer-protecting norms (provisions on labelling, advertising, packaging, consumer rights). Harmonisation also covers administrative requirements and procedures, including the application for the placement of regulated products on the market. Given such a wide range and our data-centric enquiry, our first focus will be on the general legal framework, which illustrates the global principles that frame sectoral legislation and EFSA's competences.

As mentioned in the Introduction, the General Food Law Regulation (GFLR)[94] is the cross-sectoral legislative framework in the EU food safety system. It has been drafted taking into account the 1997 Green Paper and the 2000 White Paper and sets the ground for the sectoral legislation covering specific food-related matters. Its legal bases are Articles 37, 95, 133 and Article 152(4)(b) of the Treaty establishing the European Community[95], which include objectives towards common agricultural policy, harmonisation, single market strategy and the promotion of public health. These goals are explicitly mentioned in Recital 1[96].

Following the White Paper, risk[97] analysis is tripartite[98]. Together with risk management[99] and risk communication[100], 'risk assessment' is defined as "a scientifically based process consisting of four steps: hazard identification, hazard characterisation, exposure assessment and risk characterisation" (Article 3(11) of the GFLR).

Interestingly, the precautionary principle is codified - for the first time in a normative statement (Rusconi, 2016) - in the Regulation. Article 7(1) of the GFLR states that, "in specific circumstances where, following an assessment of available information, the possibility of harmful effects on health is identified but scientific uncertainty persists, provisional risk management measures necessary to ensure the high level of health protection chosen in the Community may be adopted, pending further scientific information for a more comprehensive risk assessment". Article

[94] Regulation (EC) No 178/2002 [2002] OJ L 31/1

[95] Consolidated Version of the Treaty establishing the European Community [2002] OJ C 325/33

[96] Recital 1 of the GFLR: [t]he free movement of safe and wholesome food is an essential aspect of the internal market and contributes significantly to the health and well-being of citizens, and to their social and economic interests

[97] Article 3(9) of the GFLR: 'risk' means a function of the probability of an adverse health effect and the severity of that effect, consequential to a hazard;

[98] Article 3(10) of the GFLR: 'risk analysis' means a process consisting of three interconnected components: risk assessment, risk management and risk communication; Recital 7 of the GFLR: Where food law is aimed at the reduction, elimination or avoidance of a risk to health, the three interconnected components of risk analysis — risk assessment, risk management, and risk communication — provide a systematic methodology for the determination of effective, proportionate and targeted measures or other actions to protect health

[99] Article 3(10) of the GFLR: 'risk management' means the process, distinct from risk assessment, of weighing policy alternatives in consultation with interested parties, considering risk assessment and other legitimate factors, and, if need be, selecting appropriate prevention and control options

[100] Article 3(13): 'risk communication' means the interactive exchange of information and opinions throughout the risk analysis process as regards hazards and risks, risk-related factors and risk perceptions, among risk assessors, risk managers, consumers, feed and food businesses, the academic community and other interested parties, including the explanation of risk assessment findings and the basis of risk management decisions

7(2). specifies the need of these measures to be necessary and proportionate[101]

While the precautionary principle is still a guiding principle for risk managers, it illustrates the necessary interplay between risk assessment and risk management with the latter being directly influenced by the quality ("nature of the risk to life or health") and quantity ("the type of scientific information needed") of scientific uncertainty. As risk managers *may* take measures on the basis of the precautionary principle, such interplay cannot be deemed as a necessary dependence. If we include the principle of proportionality and the temporal constrains to adopt measures, we can notice that a reasonable margin of discretion is still granted to risk managers in spite of the bindingness of the precautionary principle.

EFSA, data collection and storage

Let us now turn to the establishment of EFSA and its task. Chapter III of the GFLR is dedicated to its mission and its internal organisation. Article 22 attributes the risk assessment competences (Paragraph 2) and requires their independent fulfilment (Paragraph 7). EFSA's tasks are listed Article 23. In addition to the drafting of the "best possible scientific opinions" (Article 23(a)) and support activities to risk management, they include the duty to "search for, collect, collate, analyse and summarise scientific and technical data in the fields within its mission" (Article 23(c)).

Then, Article 33(1) details the information-types that EFSA has to collect:

- food consumption and the exposure of individuals to risks related to the consumption of food;
- incidence and prevalence of biological risk;
- contaminants in food and feed;
- residues.

Paragraphs 2 and 3 of Article 23 sets further provisions regarding the collabora-

[101] Article 7(2) of the GFLR: [m]easures adopted on the basis of paragraph 1 shall be proportionate and no more restrictive of trade than is required to achieve the high level of health protection chosen in the Community, regard being had to technical and economic feasibility and other factors regarded as legitimate in the matter under consideration. The measures shall be reviewed within a reasonable period of time, depending on the nature of the risk to life or health identified and the type of scientific information needed to clarify the scientific uncertainty and to conduct a more comprehensive risk assessment.

tion between EFSA and national authorities in Member States, which are required to transmit the data listed above to EFSA, including those coming from business organisations, academic studies and third countries. Finally, Paragraph 6 mandates that the European Parliament, the Commission and Member States shall be allowed to scrutinise EFSA's work in the field of data collection. Interestingly, "the Authority shall search for, collect, collate, analyse and summarise relevant scientific and technical data" (Paragraph 1), whereas the scrutiny of risk managers and Member States is only extended to "the results of its work in the field of data collection" (Paragraph 6). The reasons underlying this discrepancy are unclear. Perhaps, the legislator intended to broaden the scope of the "field of data collection" to include all the sets of operation listed in Paragraph 1, rather than confining the remit of assessors' oversight to the mere acquisition of data.

EFSA data transparency obligations

The provisions set out in Article 38, 39 and 41 aim to strike a balance between the clashing interests identified in the previous Chapter and in the preliminary works to the GFLR, namely the exigence of ensuring a wide dissemination of data and the protection of commercial interests of private parties. These provisions need a careful scrutiny because the balance of interests and its further developments raise questions of interest in the field of data ownership to which attention will be devoted in this Chapter.

While the Green Paper conceptualised transparency as a principle governing the processes upon which risk assessment is based, the White Paper extended its scope to the internal discussion in the drafting steps of scientific opinions, food safety legislation, internal organisational measures and publications of documents online. The only reference to the dissemination of data ("widest possible") was contained in the intermediary Medina Report, truly a critical document focused on allegedly non-independent risk assessment conducts taken by risk managers during the BSE. The approach taken by the GFLR takes into account this evolution while constraining the remit of data dissemination to guarantee the protection of business operators and market players.

Article 38(1) lists the kind of document that EFSA has to make public without delay. Together with internal agenda and minutes (lett. a), scientific opinions adopted by the Scientific Committee and the Scientific Panels (lett. b), declarations of interests (lett. d), annual reports (lett. e), and amendments to requests to scientific opinions from the European Parliament, the Commission or Member States (lett. f), two data-related kinds of documents have to be published for transparency reason:

- The information on which its opinions are based, without prejudice to Articles 39 and 41 discussed below (lett. (c)). The identification of this information is *prima facie* unclear. Several interpretations of the notion of information - ranging them from the literature on a given topic to the personal notes of scientists involved in the studies - might be proposed. In particular, should raw data be included among the information on which EFSA opinions are based? Two answers, equally right in principle, should be investigated. On the one hand, our technical literature review has suggested that data are epistemically functional to generate scientific evidence and hence a positive answer regarding the possible inclusion should be given; on the other hand, a negative answer might depend on a narrow interpretation of the term "information" which is inextricably linked to the level of abstraction of an epistemic agent (§1.2.3), thus preventing the inclusion of raw data for being devoid of any semantic value.

- The results of its scientific studies (lett. (e)); similarly to the previous point, questions about the information to be disclosed can be raised. In particular, shall derivative and inferred data be considered "results" of EFSA scientific studies for the purposes of publication? Some might advocate that the remit of "results" should be confined to the epistemic conclusions reached by EFSA after its studies, whereas others could argue that data analysis generates outputs that are different from scientific evidence nonetheless to be published for their instrumentality to a transparent and accountable risk assessment.

EFSA confidentiality management

Leaving temporarily aside these questions, it is time to focus on the remit of confidentiality as defined by Article 39 of the GFLR. The general principle is enshrined in Paragraph 1: "[b]y way of derogation of Article 38, the Authority shall not divulge to third parties confidential information that it receives for which confidential treatment has been requested and justified, except for information which must be made public if circumstances so require, in order to protect public health". A literal interpretation of the provision suggests that the secrecy of confidential information that does not belong to the Authority is 1) a derogation to the general principle of transparency and 2) subordinate to the protection of consumers' health.

EFSA is competent for the evaluation on confidentiality claims, decided according to an internal procedure that assesses the circumstances of individual claims brought by companies (Article 39(1)). This internal procedure for the handling of confidentiality claims is regulated within the general Guidance for the application for regulated products (EFSA, 2018a, para 2.15). The factors to be taken into account are: whether the information claimed to be confidential is available only to a limited number of individuals, and is not publicly available (*secrecy of the information*); whether the disclosure of the information at stake will result in serious harm to the interests of the person who has provided it or to third parties (*harmfulness* *of the disclosure*); whether the interests claimed to be harmed by the disclosure of the information at stake are worthy of protection *(worthiness of the interests*). The cited reference guide includes data (globally referred to as "information" or "scientific information") among the documents to be submitted.

Article 41(1) states that Regulation 1049/2001[102] shall apply to documents held by the Authority, which in turn is obliged to adopt by reactive transparency measures (Art. 31(2)). In addition to these implementations, in 2015 EFSA decided to proactively open a portion of its Data Warehouse to the public (EFSA, 2015d), following the access rules discussed in § 2.2.1. In 2019, EFSA has strengthen proactive disclosure of data via Zenodo - Knowledge Junction[103]. This platform is also used to identify metadata that contribute to data standardisation, as with the case of dietary and background information metadata referred in Table 6.4.

In summary, the GFLR lays down several rules concerning the collection and dissemination of personal and non-personal data, to be read within the context of risk analysis (i.e. assessment, management and communication) and in light of the precautionary principle (i.e. uncertainty of risks entails cautious measures to be taken) and communication duties, including in the case of scientific uncertainty. This legislative framework has also been drafted under the umbrella concept of "transparency", which is also the heading of Article 38 of the GFLR. This principle has multiple facets, which include fostering trust in the institution (Recital 9 of the GFLR), contributing to risk assessment via scientific studies (Article 9 of the GFLR), fostering a democratic oversight over decision-making processes (Article 10 of the GFLR)[104].

The 2002 version of the GFLR is not exempt from a high margin of discretion in assessing the secrecy of information, the harmfulness of data publication and the worthiness of the interests underlying the non-disclosure of data, namely the three criteria that lead to a given decision on confidentiality. This might be due to the necessity of preserving flexibility when managing confidentiality requests or preventing conflicts thanks to a progressive dialogue between food business operators applying to authorisations and the Authority. However, flexibility makes it hard to foresee the outcome of the confidentiality claim (which is detrimental for the industry) and the negotiation, in the absence of a public *ex ante* scrutiny, leaves citizens with little o no oversight over the whole process. The exercise of discretionary powers by EFSA has also led to claims brought before the ECJ, whose outcomes

[102] Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents [2001] OJ L145/43

[103] https://zenodo.org/communities/efsa-kj/?page=1

[104] §3.3 of this Chapter will discuss the perspectives given by the European Court of Justice when identifying these rationales

are discussed later on in this Chapter. Instead, the next section will discuss the 2019 amendments to the GFLR that directly tackles these issues.

3.1.3 The latest EU reform: The Transparency Regulation (Reg. 2019/1381)

The concerns highlighted in the previous section were confirmed by the 2018 Fitness Check of the General Food Law[105]. The initiative has been launched as a reply to the citizens' legislative initiative ”Ban Glyphosate and Protect People and the Environment from Toxic Pesticides”[106] in the aftermath of the Monsanto Paper scandal mentioned in §2.4.3. Organisers collected 1,070,865 signatures. In summary, the petition contained:

(a) a proposal for a ban of glyphosate-based herbicides due to their carcinogenicity;

(b) a provision shifting the burden to prove the safety of regulated products for market approval from industry-led studies to institution-commissioned studies;

(c) the progressive reduction of pesticides use in the EU.

The Fitness Check covered a wide range of topics, including the perceived effectiveness of the principle of transparency (Bartl, 2015). The outcome was straightforward and it is worth quoting the Executive Report of the Fitness Check[107] in its entirety: "[d]espite overall considerable progress, transparency of risk analysis remains an important issue in terms of perception: as regards risk assessment in the context of authorisation dossiers, EFSA is bound by strict confidentiality rules and by the legal requirement to primarily base its assessment on industry studies, laid down in the GFLR and in the multiple authorisation procedures in specific EU food legislation. These elements lead civil society to perceive a certain lack of transparency and independence, having a negative impact on the acceptability of EFSA's

[105] EU Commission, 'REFIT Evaluation of the General Food law (Regulation (EC) No 178/2002' SWD(2018) 38 final, available at https://ec.europa.eu/food/sites/food/files/gfl_fitc_comm_staff_work_doc_2018_part1_en.pdf

[106] The official registration was recorded in the Communication of the Commission on the European Citizens' Initiative "Ban glyphosate and protect people and the environment from toxic pesticides", available at https://ec.europa.eu/transparency/regdoc/rep/3/2017/EN/C-2017-8414-F1-EN-MAIN-PART-1.PDF

[107] https://ec.europa.eu/food/sites/food/files/gfl_fitc_executive_summary_2018_en.pdf, page 3

scientific work by the general public. There is therefore a need to address these issues in order to protect the reputation of EFSA's work". The full report clarifies how NGOs criticise that 1) raw data are not made available due to confidentiality rules, thus making access to studies excessively restrictive, 2) secondary food legislation sets further confidentiality restriction, and 3) that the combination of a general legal framework, secondary legislation and access to documents rules make "create a rather complex system for the public release of documents"[108].

In its reply to the "Ban Glyphosate" initiative, the Commission stated that "[t]he Commission will propose changes to the legislation to increase the transparency of studies commissioned by industry that are submitted in application dossiers, while respecting the principles set in the Treaty regarding the protection of legitimate confidential business information, including measures such as public access to raw data from study reports, thus reducing the need for stakeholders to have recourse to access to documents procedures".

The Transparency Regulation, i.e. Regulation 2019/1381[109] consists of a set of amendments to the GFLR and sectoral legislation. The reform heavily amends transparency provisions and the data submission procedure. The first proposal from the Commission was published on 11 April 2018 and it was finally approved on 20 June 2019. Provisions will enter into force on 27 March 2021.

The table below shows a direct comparison between the pre-reform version of the GFLR and the amendments brought by the Transparency Regulation.

Table 3.1: Table:3.1 - GFLR and Transparency Regulation

GFLR Article	Transparency Regulation Article	Heading
32	32 (not replaced)	Scientific studies
	32a	Pre-submission Advice
	32b	Notification of studies
	32c	Consultation of Third Parties

[108] See n. 105, p. 35

[109] Regulation (EU) 2019/1381 of the European Parliament and of the Council of 20 June 2019 on the transparency and sustainability of the EU risk assessment in the food chain and amending Regulations (EC) No 178/2002, (EC) No 1829/2003, (EC) No 1831/2003, (EC) No 2065/2003, (EC) No 1935/2004, (EC) No 1331/2008, (EC) No 1107/2009, (EU) 2015/2283 and Directive 2001/18/EC [2019] OJ L231

	32d	Verification Studies
33	33	Collection of data
34-37 (not replaced)		
38	38 (replaced)	Transparency
39	39 (replaced)	Confidentiality
	39a	Confidentiality Request
	39b	Decision on Confidentiality
	39c	Review of Confidentiality
	39d	Obligations with regard to Confidentiality
	39e	Protection of Personal Data
	39f	Standard data formats
	39g	Information systems

New Articles 32a "Pre-submission advice", 32b "Notification of studies", 32c "Consultation of third parties", 32d "Verification studies"

New articles 32a, 32b, 32c, 32d have been inserted. In the context of applications for regulated products, the Authority is now competent for giving advice on "the rules applicable to, and the contents required for, the application or notification, prior to its submission" (New Art. 32a(1)), including via its website (New Art. 32a(2)). Article 32b(1) establishes a a database of studies commissioned or carried out by business operators prior to the application. Undertakings shall notify the Authority of the scope of the study, without delay (New Art. 32b(2)). Vice versa, laboratories shall notify EFSA the mandate to carry out studies (New Art. 32b(3)). The notification of the study is a mandatory requirement within the application procedure, even though remission mechanisms allow the re-submission (New Articles 32b(4), 32b(5)). New Art. 32c provides for a consultation mechanism in the case of a renewal of an application/authorisation[110]. When this is the case, EFSA has to launch a "consultation of stakeholders and the public on the intended studies for renewal, including on the proposed design of studies" following the notification of the studies (New Art. 32c(1)). Access to data by these third parties is granted only to the non-confidential version of the application dossier as described below

[110] As observed in §2.4.2, certain regulated products (e.g. GM food and feed) are subject to a mandatory renewal procedure after a certain amount of years (e.g. 10 years for Genetically Modified food (Art 7(5) of Regulation 1829/2003 (see below))

(New Art. 32c(1)). Consultation has to occur immediately after the disclosure of the dossier "in order to identify whether other relevant scientific data or studies are available on the subject matter concerned". New Article 32d allows the Commission to authorise EFSA to commission independent studies in exceptional circumstances of serious controversies or conflicting results. This provision might be deemed as the acceptance of petitioners' claims for more independence from the industry by EFSA. However, as these independent studies are limited to cases of scientific uncertainty - which might also emerge from *ex post* studies rather that prior research as observed in IARC case - and subject to budget constraints, the efficacy of Article 32d can be challenged.

Amended Article 38 "Transparency"

Article 38(1) has been significantly amended by several new provisions. For what concerns data "proactive" publication, subheadings specify the scientific information-types to be published:

- b) EFSA scientific outputs, including the opinions of the Scientific Committee and the Scientific Panels after adoption, minority opinions and results of consultations performed during the risk assessment;
- c) Scientific data, studies and other information supporting applications, including supplementary information supplied by applicants, as well as other scientific data and information supporting requests from the European Parliament, the Commission and the Member States for a scientific output, including a scientific opinion;
- d) Information on which EFSA scientific outputs, including scientific opinions, are based;
- f) EFSA scientific studies in accordance with Art. 32 and new Art. 32d

The first three provisions mentioned above include a "taking into account the protection of confidential information and the protection of personal data in accordance with Articles 39 to 39e" clause, whose implications and mechanisms will be discussed below. Information shall be made public without delay, with the exception of scientific data under letter c) which shall be made public without delay once an application has been considered valid or admissible. Scientific outputs under letter b) have to be made public in a dedicated section of the Authority's website open and accessible to the public. They also have to be downloadable, printable and indexed.

With particular regard to data disclosure under letters (c) and (d)), new provisions in the new Paragraph 1a of Article 38 include the protection of:

- (a) existing rules concerning intellectual property rights which set out limitations on certain uses of the disclosed documents or their content;
- (b) any provisions set out in Union law protecting the investment made by innovators in gathering the information and data supporting relevant applications for authorisations (“data exclusivity rules”)

Finally, Article (38.1a) sets out that the disclosure to the public of information "shall not be considered to be explicit or implicit permission or licence for the relevant data and information and their content to be used, reproduced, or otherwise exploited in breach of any intellectual property right or data exclusivity rules, and the Union shall not be responsible for its use by third parties. The Authority shall ensure that clear undertakings or signed statements are given to that effect by those who access the relevant information prior to its disclosure".

Amended Article 39 "Confidentiality"

The amended version of Article 39 opens with a reaffirmation of the exceptional nature of confidential treatment over submitted information (Paragraph 1). New Paragraph 2 imposes on applicants the burden to prove that the disclosure of the information at stake can potentially harm their interests. Moreover, it clarifies the information-types for which confidential treatment can be requested. Together with information on applicant’s manufacturing processes and methods, commercial relationships and business strategy, lett. d) extends the scope of confidentiality requests to the quantitative composition of the subject matter of the request, except for information which is relevant to the assessment of safety. Paragraph 3, allows derogations of confidentiality rules to be implemented by EU food sectoral legislation. Paragraph 4, derogates to the list of paragraph 2 in the event of urgent actions to protect animal health or the environment or if the information at stake is the basis of a scientific output, including opinions, issued by the Authority when effects on the same subject are foreseeable.

New Articles 39a "Confidentiality request", 39b "Decision on confidentiality", 39c "Review of confidentiality", Article 39d "Obligations with regard to confidentiality"

Articles inserted after Article 39 clarify the mechanism of the confidentiality request. Most notably, new Articles 39a provides that applicants requesting confidential treatment have to submit a non-confidential version of the dossier devoid of information deemed worth of confidentiality and elicited as missing. The full and confidential version shall also be submitted, with allegedly confidential information clearly marked.

New Article 39b sets out the general procedure to follow when the Authority handles confidentiality requests, as the figure below displays in a simplified and accessible form. Together with the examination of the confidentiality requests, the publication of the non-confidential version of the dossier occurs without delay following the submission. The dialogue between applicants and EFSA is now regulated according to a precise timeline.

Additional data can also be submitted during the procedure. However, this does not hamper their publication: as a general rule of thumb, all the data for which confidentiality requests or claims have been rejected have to be made public, either without delay or following a "cooling-down period" given to the applicant to reason about its next steps. Remarkably, reasoned decisions taken by EFSA can be now challenged before the Court of Justice (New Article 39b(3)).

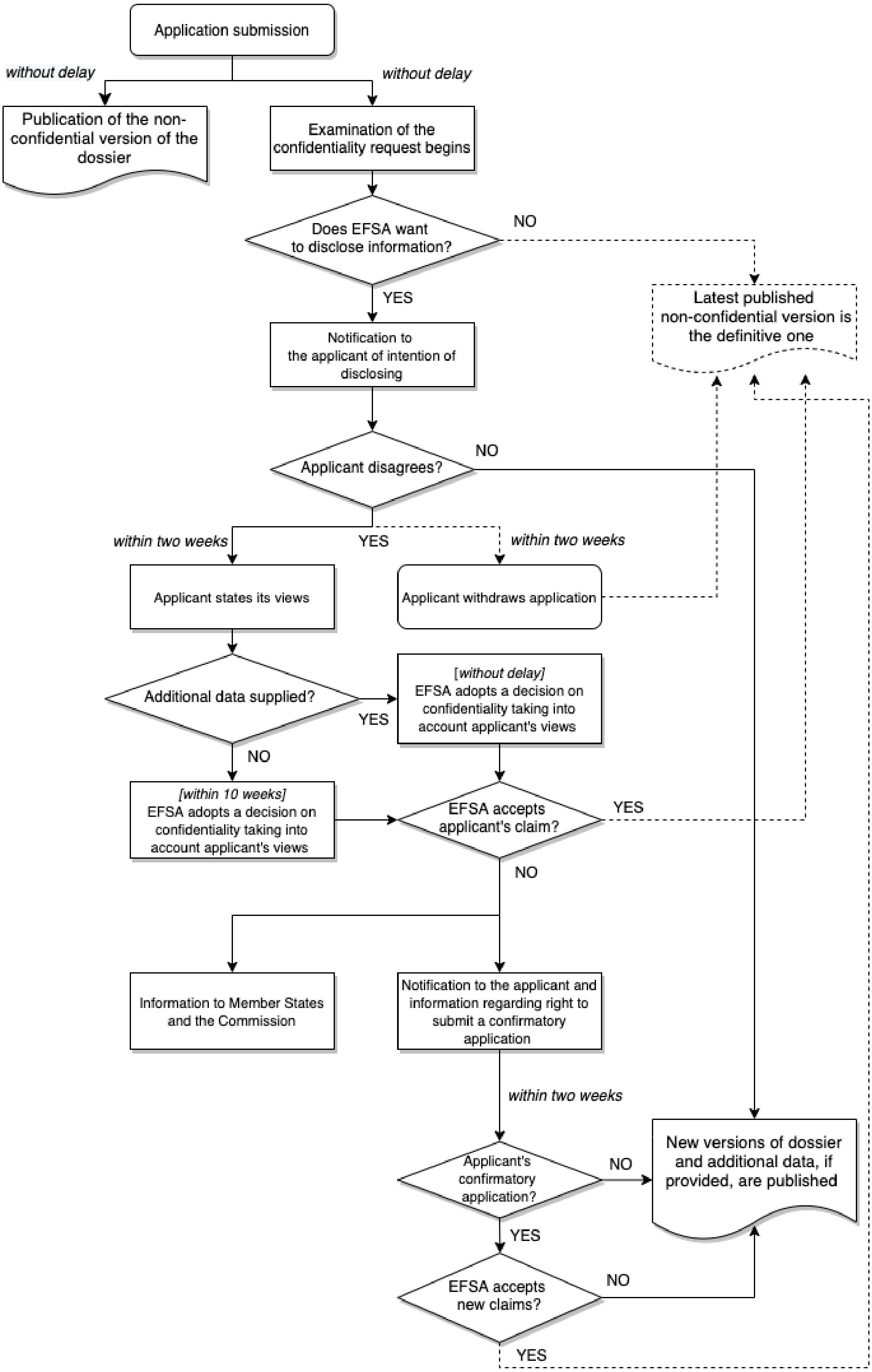

Application submission
without delay
without delay
Publication of the non-confidential version of the dossier
Examination of the confidentiality request begins
Does EFSA want to disclose information?
NO
YES
Latest published non-confidential version is the definitive one
Notification to the applicant of intention of disclosing
Applicant disagrees?
NO
within two weeks
YES
within two weeks
Applicant states its views
Applicant withdraws application
Additional data supplied?
YES
[without delay] EFSA adopts a decision on confidentiality taking into account applicant's views
NO
[within 10 weeks] EFSA adopts a decision on confidentiality taking into account applicant's views
EFSA accepts applicant's claim?
YES
NO
Information to Member States and the Commission
Notification to the applicant and information regarding right to submit a confirmatory application
within two weeks
Applicant's confirmatory application?
NO
New versions of dossier and additional data, if provided, are published
YES
EFSA accepts new claims?
NO
YES

Figure 3.1: Confidentiality requests management process (New Art. 39b GFLR)

Article 39c states that EFSA has to periodically review confidentiality decisions whether conclusions of scientific outputs, including scientific opinions, highlight foreseeable effects on human and animal health or on the environment and the previously confidential information has to be made public[111]. When this is the case, Article 39b applies.

Article 39d consists of a series of additional provision regarding confidentiality, e.g. for what concerns staff and managers or in the case of withdrawal of application. In relation to the procedure set out in Article 39b, new Article 39d(2) clarifies that information on which confidentiality request has been submitted shall not be made available to the public until a final decision has been reached. Likewise, the Commission and the Member States shall make efforts to prevent the publication of information for which confidentiality has been accepted.

On March 2020, EFSA published a working document on practical arrangements on Articles 38 and 39[112]. Despite not representing the official position of the Authority, it offers a preliminary scrutiny over the implementing measures that EFSA might adopt in compliance with the Transparency Regulation. Paragraph 8 of the draft implementing practical arrangements lists the content of confidentiality requests, i.e. a clear indications of documents, information or data for which confidentiality request can be requested and which explanation/justification applicants shall provide to obtain the confidential status. In particular, applicants should prove:

- The secrecy of the information, to be intended as the lack of public availability.
- A potential significant harm of the disclosure, equivalent to the 5 percent of the total turnover for legal persons or earnings for natural persons. If this requirement is not met, a documented justification of the potential or foreseeable harm to applicant's interests has to be submitted;
- The worthiness of protection for the concerned data;
- The confirmation that document, information or data, have been finalised within 5 years prior to the submission. If this requirement is not met, a specific justification of the potential harm to applicant's interests has to be attached.

[111] This new provision mirrors "reactive" transparency measures mandated by Regulation 1049/2001 as amended by the Aarhus Regulation. These measures will be discussed in §3.3

[112] https://ec.europa.eu/food/sites/food/files/safety/docs/gfl_expg_20200303_efsa.pdf

The European Crop Protection Association (ECPA)[113] published its legal analysis of the draft practical arrangements[114]. ECPA noted that 1) EFSA might have set a threshold (5 percent) which cannot contemplate the loss in the competitive position of the applicant and the competitive advantage to competitors since they are too difficult to calculate prior to the disclosure of data, and 2) EFSA might have exceeded the scope of the Transparency Regulation when setting the "not older that 5 year" requirement to assess the novelty of document, information and data. This latter requirement also allegedly lacks of a clearly identified rationale that links the 5-year timespan to the presumption of a harmless disclosure.

New Article 39e: "Protection of personal data"

Article 39e regards the protection of personal data. However, the information that the legislator mainly intended to protect is of a different kind than the one highlighted in Chapter II. In fact, Article 39e regulates the processing of four different kinds of information:

- information pertaining the name and address of the applicant, author(s) of supporting studies, participants and observers of working groups and scientific panels. For transparency reasons, these names have always to be made public.

- names and addresses of natural persons involved in testing on vertebrate animals or in obtaining toxicological information. The disclosure of this information is deemed to significantly harm the privacy and the integrity of these individuals, so it should not made public unless differently specified by Regulation 2018/1725[115], which balances the protection of personal data processed by EU bodies and institutions with the general access to the same information by the public for reasons of transparency[116].

[113] The European Crop Protection Association (ECPA) represents crop protection industry in the EU. It is registered in the EU Transparency Register (ID: 0711626572-26) among the trade and business associations, It promotes the "the scientific study and analysis of all fields of interest to the crop protection industry"

[114] https://ec.europa.eu/food/sites/food/files/safety/docs/gfl_trans-reg_impl-feedback_laeg-analy_20200323.pdf

[115] Regulation 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295/39

[116] The reason underlying this provision is that "[u]nfortunately, a minority of individuals who oppose the use of animals in research have used threats and even terrorism to further their views" (Beversdorf et al., 2015) against researchers

- any personal data made public pursuant to Article 38 GFLR[117]. The divulgation of this data shall only be used to ensure the transparency of the risk assessment. A clear reference to the necessary compatibility of the secondary processing is provided by an explicit mention and Article 4(1)(b) of Regulation 2018/1725.

- any other personal data the processing of which is carried out pursuant the GFLR (residual clause). This processing of this information by EFSA falls under the regime of Regulation 2018/1725.

The new provision on personal data seems to be mainly focused on the names of individuals working within the remit of risk assessment activities or other scientists involved in testing. However, we noted that EFSA also collects personal food consumption data and background information at individual level via Member States and makes them available though its Food Consumption Database in aggregated forms. The legal regime for the processing of this information is the one enshrined by the last point mentioned above, which covers *any* personal data processed in the context of the GFLR. It might be questioned whether or not this regime also applies to commercial applicants[118]. Following a literal interpretation of Article 39e, an affirmative answer should be given insofar the statement "the processing of personal data carried out pursuant" the GFLR is interpreted broadly. However, this would imply the extension of Regulation 2018/1725 beyond its scope (Article 2 of Regulation 2018/1725)[119], thus a cautious answer making the GDPR alone applicable to commercial applicants that operate within the material and territorial scope of the GDPR should be preferred.

In the previous Chapter, we noted that trends in food consumption data gathering reveal a higher degree of proximity to the data subject in comparison to traditional methods and the collection of background information is, in general, not exempt from risks[120]. However, these risks emerging from this data processing are balanced by the adoption of pseudonymisation techniques by EFSA (EFSA, Du-

[117] Article 38 contains few explicit examples of personal data: participant lists (Article 38(1)(a)) and declarations of interest (Article 38(1)(e)) made by the members of EFSA working groups and scientific panels, authors of the scientific opinions (Article 38(1)(b))

[118] It could be assumed that applicants for regulated products authorisation usually qualify as data controllers, whereas external laboratories to whom analysis is delegated should be deemed as data processors operating on behalf of the applicant under a data processing agreement

[119] Article 2(1) of Regulation 2018/1725: [t]his Regulation applies to the processing of personal data by all Union institutions and bodies

[120] Recital 46 of Regulation 2018/1725 specifies the extent to which certain data processing activities might results in risks for individuals. *Inter alia*, risks could emerge from the processing of children's personal data, a large amount of personal data (see also Table 6.4) or a large number of data subjects. These three conditions are met in food consumption and background information processing

jardin, et al., 2019, p.13, p.19), a suitable safeguard measure according to Articles 13, 27, and 33 of Regulation 2018/1725. It is worth noticing that Member States adopted jeopardised data protection measures when building national datasets. For instance, Spain simply treated personal data "as confidential" (Marcos et al., 2016, para 2.6)[121], France had to obtain a mandatory authorisation by the French Data Protection Authority (Dubuisson et al., 2017, para 2.6), the Netherlands did not report about data protection aspects (Public Health et al., 2018, para 2.6), Italy stated that "[t]he survey was exclusively observational and non-invasive, ethical aspects were related only to the collection of information on food habits that may be related to health and thus might be sensitive. INRAN is part of the National Statistical System (SISTAN) and guarantees individual data protection. An additional ethical committee review of the study protocol was considered unnecessary" (Sette et al., 2011, p.923). Remarkably, datasets generated by these studies and made available to EFSA include both dietary intake and background information, as established by the guidelines discussed in the previous Chapter (EFSA, 2014a, ch. 7).

The dishomogeneity in addressing data protection concerns can be due to multiple reasons including: a) the wide time span in which data collection has been performed, which imply the shift from the Data Protection Directive to the GDPR in Member States legislation; b) the lack of a uniform guidance on key aspects regarding the essential data protection regime for food consumption data collection across the Member States; c) the derogation allowed by the GDPR for research and statistical purposes to be implemented by national laws (Article 89 GDPR). Moreover, EFSA 2019 decision on the processing of personal data[122] is not decisive in solving data protection concerns since it places risk assessment outside of its scope[123].

[121] In the context of food safety risk assessment data, the use of such wording might be misleading. As we noted, confidentiality regime applies to information submitted in the context of regulated product and confidentiality is granted after the scrutiny illustrated above. It might be the case that "as confidential" is a communicative substitute for "in compliance with data protection law" that has been used when informing participants on matters related to data protection. However, such wording does not offer us any possibility to review the extent to which the data controller has addressed data protection issues

[122] Decision of the European Food Safety Authority of 19 June 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of EFSA (2019) OJ L 272/154

[123] Article 2(2) of the Decision: [w]ithin the framework of the administrative functioning of EFSA, this Decision applies to the processing operations on personal data by EFSA for the purposes of conducting administrative inquiries, disciplinary proceedings, preliminary activities related to cases of potential irregularities reported to OLAF, processing whistleblowing cases, (formal and informal) procedures of harassment, processing internal and external complaints, conducting internal audits, investigations carried out by the Data Protection Officer in line with Article 45(2) of Regulation (EU) 2018/1725 and (IT) security investigations handled internally or with external involvement (e.g. CERT-EU)

New Article 39f "Standard data formats", Article 39g "Information systems"

Transparency Regulation also intervenes on standardisation of data formats. It is required that the Authority and the Commission cooperate to draw formats that are not based on proprietary standards, are capable of ensuring interoperability with the state-of-the-art (as described in the previous Chapter) and suits the need of small and medium-sized enterprises. The adoption of standardised data formats is then detailed in sectoral legislation.

Finally, new Article 39g prescribes the use of auditable and secure information systems by EFSA, specifically to protect personal and confidential data.

3.2 EU Sectoral legislation

EU food sectoral legal system consists of several pieces of legislation that integrate the GFLR to tackle specific issues (including advertisement, labelling, packaging, and so on) and setting strict harmonised security standards for foodstuffs and food supplements (Sachs, 2016). The alignment of the GFLR to sectoral legislation is also true as regards data-related provisions.

As noted above, new Article 38(1a) leaves room for the adoption of derogatory measures in sectoral legislation aiming at regulating scenarios in which the "transparency *vs* confidentiality" debate is more polarised due to multiple reasons, such as the turnover in lucrative market sectors or the scientific uncertainty surrounding certain products. The Transparency Regulation has also amended sectoral legislation to make it consistent with the general framework, thus making legal scrutiny necessary to detail the general picture introduced in the previous section. The rationale underlying each focus is described in each paragraph.

3.2.1 Regulation 1829/2003 on Genetically Modified food and feed

Genetically Modified (GM) food and feed contain or consists of artificially-modified organisms usually referred to as Genetically Modified Organisms (GMOs), which present genetic modifications made possible by gene editing[124]. Such interventions

[124] Article 2(2) of Directive Directive 2001/18/EC of the European Parliament and of the Council of 12 March 2001 on the deliberate release into the environment of genetically modified organ-

allow for desirable properties given by modified proteins, including the resistance to certain disease or an increased productivity". Ethical controversies on the use of gene editing arose in 1977 with Jeremy Rifikin's book "Who should play God?" (Rifkin and Howard, 1977) and continued covering a wide range of topics: from the patentability of GMOs, to scientific controversies regarding their safety, to possible threats to biodiversity (Jasanoff, 2016; Schleissing et al., 2019). The EU regulatory approach has reflected this debate by setting a strict and rather complex authorisation procedure scheme for the risk assessment, which is carried out on a case-by-case approach (Regulation 1829/2003[125]), while allowing Member States to further restrict or prohibit the cultivation of GMOs in their territory (Directive 2015/412[126]).

Our analysis will be focused on the transparency of information provided by commercial applicants in the course of their authorisations at the EU level only. It has to be preliminary observed that the costs associated to the discovery, development and authorisation of a new plant biotechnology were calculated on a sum around $ 130m in 2011, spread across 15 years of investments from discovery to launch (McDougall, 2011)[127]. Regulation 1829/2003 has been amended by the 2019 Transparency Regulation and it now reflects the new approach supporting a transparent risk assessment, which is particularly significant in light of the relevant costs associated to the discovery and development of GM food and feed.

isms and repealing Council Directive 90/220/EEC [2001] OJ L 106: "genetically modified organism (GMO)" means an organism, with the exception of human beings, in which the genetic material has been altered in a way that does not occur naturally by mating and/or natural recombination. In the recent Case C-528/16 (*Confédération paysanne and Others*), the European Court of Justice included organisms obtained by means of novel techniques of mutagenesis within the remit of the definition of GMOs due to their result in genetic modifications (paras 32 - 38), while also stating its difficulty in interpreting an outdated provision (para 47)

[125] Regulation (EC) No 1829/2003 of the European Parliament and of the Council of 22 September 2003 on genetically modified food and feed [2003] OJ L268/1

[126] Directive (EU) 2015/412 of the European Parliament and of the Council of 11 March 2015 amending Directive 2001/18/EC as regards the possibility for the Member States to restrict or prohibit the cultivation of genetically modified organisms (GMOs) in their territory [2015] OJ L68/1

[127] This study was commissioned by CropLife International, a trade association of companies active in the market of agrochemicals. BASF Corporation, Bayer CropScience, Dow AgroSciences, DuPont / Pioneer Hi-Bred, Monsanto Company, Syngenta AG have participated to the survey. Other independent studies have found higher costs due to regulatory restrictions (Bernauer et al., 2011)

Inside of a GM food application: Maize 4114

A coincise description of EFSA risk assessment opinion on Maixe 4114 (EFSA, Naegeli, et al., 2018), developed by DuPont (Pioneer Hi-Bred International Inc.) can serve as a practical reference for our investigation. The introduction of four genes (cry1F, cry34Ab1, cry35Ab1, pat) granted maize the ability to be resistant to colopteran and lepidopteran insects, as well as tolerant to glufosinate-based herbiced. EFSA concluded that "maize 4114 is as safe as the non-GM comparator(s) and non-GM reference varieties with respect to potential effects on human and animal health and the environment".

Following the description of data and methodologies used (para 2), the assessment is carried out by a systematic literature review and a qualitative description of the results ([EFSA] "GMO Panel considered the relevant publications retrieved through the literature searches and their implications for risk assessment, and addressed those in the related sections below, as appropriate") (para 3(1)). Characteristics of Maize 4114 are then presented (paras 3.1 and 3.2). Para 3.4 consists of the food and feed assessment. Toxicology tests made by the applicant are reported[a], described and reviewed[b]. Even thought in the specific case, maize is not considered to be a common allergenic food, allerginicity tests are usually recommended. Human and animal dietary assessment is carried out in para 3.4.5. Focusing on human dietary exposure, it is reported that data were provided by the applicant for age classes. Since no data on Maize 4114 were available, applicants have relied on consumption of commodities (e.g. corn bread, corn flakes) containing conventional maize. Consumption data at individual level (aggregated during the analyses) have been gathered from the EFSA Food Consumption Database. Acute and chronic exposure are calculated, while main contributors to the exposure (popcorn for acute exposure, snacks and popcorn for chronic exposure) are identified. Finally, enviromental risk assement and post-market monitoring plans are reported.

Comments following public consultation have criticised EFSA under many profiles[c]. Reviews mainly came from GMO-free organisations, which complained poor data quality, the absence of systematic literature review[d] and insufficiencies in monitoring plans.

[a] p.13: "[i]n accordance to Regulation (EU) No 503/2013, the applicant provided a 90-day oral repeated-dosetoxicity study on whole food and feed from maize 4114 in rats. Animal feeding studies in broiler and channel cat fish fed diets containing maize 4114 material were also provided in compliance with Regulation (EU) No 503/2013. All these studies were evaluated by the GMO Panel."

[b] p.15: [t]he GMO Panel noted that the applicant only tested one dose level. However, the dose tested wasclose to the highest possible without inducing nutritional imbalance according to the currentknowledge, and in accordance to the limit test dose as described in OECD TG 408. This is considerednot to compromise the study.The GMO Panel concluded that no maize 4114-related adverse effects were observed in this study after a 90-day administration to rats of a diet formulated with 32% milled grain from maize.

[c] https://ec.europa.eu/food/sites/food/files/plant/docs/plant_gmo-public_consultations-comments_maize-4114.pdf

[d] In its opinion, EFSA had stated that a literature review would not have been justified due to the paucity of sources on Maize 4114 (para 3)

The authorisation procedure consists of three steps. First, an application has to be submitted to the national competent authority of a Member State (Article 5(2)), which informs and transmit the application to EFSA (Article 5(2)(iii)). The European Authority has to inform the other Member States and and the Commission, before publishing an opinion based on the submitted data and documents (Article 6), on the basis of which the Commission has to take a formal decision on the authorisation, which remains valid for 10 years (Article 7(5)).

The authorisation dossier for GM food addressed to the Member State shall include the elements listed in Article 5(3). They encompass "a copy of the studies, including, where available, independent, peer-reviewed studies, which have been carried out and any other material which is available to demonstrate that the food complies" with safety criteria (Art. 5(3)(e)) and "either an analysis, supported by appropriate information and data, showing that the characteristics of the food are not different from those of its conventional counterpart" (Art. 5(3)(f)). The list now includes the identification of the confidential parts, accompanied by a "verifiable justification" for the confidentiality claim (amended Article 5(3)(l)). For data submissions, the use of standardised formats is now mandatory (*ex multis*, amended Article 5(3)(a), amended Article 11(2)). Equivalent provisions cover GM feed (Article 17).

Our legal focus will be on three sets of provisions, namely confidentiality, data protection[128], and specific data transmission requirements that might give rise to interpretative doubts.

For what concerns confidentiality and data protection provisions, the Preamble of Regulation 1829/2003 clarifies their rationale only for the latter, i.e. stimulating research by protecting the underlying investments (Recital 40). As regards confidentiality measures, in the absence of any explicit provision, scholars have argued that they are intended to protect the competitive position of the data originator (Holle, 2014; Simpson, 2016).

The remit of confidentiality requests has been changed from the original version of Regulation 1829/2003. In the current text, a rebuttable presumption of non-confidentiality covers information on both physico-chemical and biological characteristics of the GMO, food or feed (Article 30(3(c))) and effects of the GMO, food or feed on human and animal health ((Article 30(3(d))). Applicants have to prove that the disclosure might significantly harm their competitive position (Article 30(1)) and the Commission is charge of assessing the confidentiality claim after consultation with the applicant (Article 30(2)).

[128] As it will be noted, the meaning of "data protection" in this context - as well as in other similar domains - is different from the one attributed to measures and safeguards of personal data by (personal) data protection law

The amended version has radically changed this mechanism, First, confidentiality claims have to be handled in accordance with the provisions of the Transparency Regulation. The justification shall also be "verifiable" (as in the current version), hence the applicant carries the burden to provide additional information to justify its claims. However, references to the significant harm to applicant's competitive positions have disappeared, therefore EFSA practical arrangements and implementing rules apply in the same way of other regulated products.

The remit of confidentiality claims has also changed. From the list of elements of the current version, only items of information referred to in points (a), (b) and (c) of Article 39(2) of the amended GFLR can constitute elements of confidentiality[129]. Moreover, two specific GM-related provisions broaden the scope of confidentiality claims, which will also be able to cover:

- DNA sequence information, except for sequences used for the purpose of detection, identification and quantification of the transformation event;
- Breeding patterns and strategies.

However, this information can only be granted confidential interests only if the applicant demonstrates that the divulgation would potentially harm its interests to a significant degree, consistently with the general provision of Article 39(2) of the amended GFLR.

As regards data protection measures, Recital 40 states that their overall goal of stimulating research and development into GMOs for food and/or feed use, by protecting the investment in data gathering when supporting applications. The balance between the avoidance of repeated trials and the need to protect this investment is realized trough a limited data protection period. Therefore, article 31 ("Data Protection") has been left untouched by the Transparency Regulation. It denies a second applicant the possibility to rely on scientific data and other information provided by a previous applicant for a period of 10 years from the date of authorisation, unless they reach an agreement. Hence, in practice, the protection mechanism consists of preventing further applicants to exploit the efforts made by the first applicant in gathering data supporting its application, especially when the products to be placed in the market are essentially similar.

Commission Implementing Regulation 503/2013[130] implements Regulation 1829/2003

[129] Namely, information on applicant's manufacturing processes and methods, other than information useful for safety risk assessment (lett. a), commercial relationships (lett. b) and business strategy (lett. c)

[130] Commission Implementing Regulation (EU) No 503/2013 of 3 April 2013 on applications for authorisation of genetically modified food and feed in accordance with Regulation (EC) No

by detailing the mandatory contents of the applications to be submitted. Recital 15 of the Implementing Regulation 503/2013 states that "in order to ensure that studies are of high quality and documented in a transparent way, it is essential that they are performed under appropriate quality assurance systems[131] and raw data should be provided in all cases and be in a suitable electronic format". Therefore, Article 4 extends the submission to raw data.

Annex I and II of the Implementing Regulation detail the contents of general and scientific information to be submitted. *Inter alia*, two of them require particular attention for the purposes of our analysis:

- The submission of data on the consumption of the recipient plant (i.e. the one in which genetic modifications will occur) have to be attached. However, a specification covers the description of "the normal role of the plant in the diet (such as which part of the plant is used as a food or feed source, whether its consumption is important in particular subgroups of the population)" (point 1.1.2 of Annex II). This information is needed for hazard identification and characterisation;

- The submission of the "raw data and the programming code used for the statistical analysis" for the comparison between the genetically modified plant and its conventional counterpart (point 1.3.2.2 of Annex II).

On the one hand, the first point leaves open the question about the identification method of subgroups, since aggregation occurs at age-level as we noted in Chapter 2. This concern however, does not refer to the core topic of this Chapter, hence we will leave it temporarily aside. The second point raises issues regarding the accessibility of the source code for transparency and, broadly speaking, whether or not computer programmes used by applicants in the fields of regulated products can go under scrutiny and by whom. I will try to reply to this question at the end of this Chapter.

Raw data on GM food and feed are also subject to another piece of legislation, namely Regulation 1367/2006 ("Aarhus Regulation")[132], which transposes the Aaruhs

1829/2003 of the European Parliament and of the Council and amending Commission Regulations (EC) No 641/2004 and (EC) No 1981/2006 [2006] OJ L 157/1

[131] The Recital also specifies that principles for quality assessment of the testing facilities are laid down by Directive 2004/10/EC, which adopts good laboratory practice (GLP) standards. For testing facilities outside the EU, OECD Principles on Good Laboratory Practice (GLP) shall be followed

[132] Regulation (EC) No 1367/2006 of the European Parliament and of the Council of 6 September 2006 on the application of the provisions of the Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters to Community institutions and bodies [2006] OJ L 264/13

Convention[133] within the EU legal framework and set further obligations to Member States (all of which were already signatories of the Convention before the formal signature by the Union). Both the goal of the Convention and the Regulation is threefold: granting access to information related to emissions into environment, ensuring public participation in decision-making processes and providing access to justice in environmental matters.

As regards access to data, the Aarhus Regulation broadens the scope of Regulation 1049/2001 requests for access to environmental information specifically to include genetically modified organisms (Art. 2(d)(i)). Obligations coming from the Aarhus Regulation include the collection of "environmental impact studies and risk assessments concerning environmental elements" (Art. 4(2)(g)). Then Art. 6(1) of the Aarhus Regulation prescribes a restrictive interpretation of the grounds of restriction of access set in Art. 4(2) of Regulation 1049/2001, which includes prejudices to "commercial interests of a natural or legal person, including intellectual property".

In its working document on practical arrangements seen above[134], EFSA stated that "any information falling under the definition of “environmental information” pursuant to Article 2 of Aarhus Regulation should not be treated as confidential since, in accordance with Article 4 of this piece of legislation, the Authority is required to make such information available to the public". Expectedly, the industry has negatively assessed EFSA’s decision to deny confidentiality affirming that a) Article 4 of Aarhus Regulation concerns "reactive transparency" rather than "proactive transparency", as in the case of the amended GLFR, under whose remit confidentiality claims fall, b) that the GLFR prevails on the Aarhus Regulation as *lex specialis* and c) Aarhus Regulation explicitly mentions the aforementioned exceptions to requests to access.

Taken together, the legal framework regarding the transparency and the confidentiality of data related to GM food and feed is rather complex due to the interplay of several layers of normative interventions stratified over time. The attempt made by the Transparency Regulation is likely to be successful on the goal of harmonising the specific assessment procedure of confidentiality claims with the general framework set by the amended GFLR. However, the presence of multiple layers of regulation might hinder the harmonisation of their outcomes. EFSA tried to find a working solution by prioritising transparency for the purposes of complying with the Aarhus Regulation, but negative feedbacks from the industry have shown how this preliminary attempt has failed to provide a shared solution, also on matters of legal interpretation.

[133] Convention on Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters signed in Aarhus, Denmark, on 25 June 1998

[134] https://ec.europa.eu/food/sites/food/files/safety/docs/gfl_expg_20200303_efsa.pdf

3.2.2 Regulation 1924/2006 on Health Claims

Regulation 1924/2006[135] on Health claims has intervened to regulate assertions regarding nutritional (e.g. "low-fat", "sugar-free", etc.) or health-related (e.g. "lowers cholesterol levels", "promotes bone growth", etc.) properties of marked food (Sachs, 2016, p. 443). These rules prevent the use of claims that a) are false, ambiguous or misleading, b) give rise to doubt about the safety and/or the nutritional adequacy of other foods or encourage or condone excess consumption of a food, c) discourage balanced and varied diets, or d) depict bodily changes that might induce fears in consumers (Art. 3).

The application procedure is similar to the general framework, but it includes some caveats. Companies may apply to the competent national authorities for an authorisation to use a certain health claim, Then, the assertion is evaluated by EFSA and, on the basis of its opinion, the Commission opts to update a list of allowed claims[136]. As in the general framework, applicants carry the burden to substantiate their claims (Art. 6) and assessment shall take into account all the available scientific data (Recital 17).

Specific-data related provisions are the ones enshrined in Article 21, not amended by the Transparency Regulation. In particular, Regulation 1924/2006 contains a specific "data protection" rule which prevents further applicants to rely on the data provided by a previous applicant. Three conditions have to be met:

- scientific data and other information has been designated as proprietary by the prior applicant at the time the prior application was made (Art. 21(1)(a))
- the prior applicant had exclusive right of reference to the proprietary data at the time the prior application was made (Art. 21(1)(b))
- the health claim could not have been authorised without the submission of the proprietary data by the prior applicant (Art. 21(1)(c))

While this mechanism is similar to the provisions seen above regarding GM food and feed, this procedure can be avoided if the Commission takes a decision on whether a claim could be or could have been included in the nutrition/health claim

[135] Regulation (EC) No 1924/2006 of the European Parliament and of the Council of 20 December 2006 on nutrition and health claims made on foods [2006] OJ L 404/9

[136] Health claims are listed in an open portal set up by the EU Commission (https://ec.europa.eu/food/safety/labelling_nutrition/claims/register/public/?event=search) similarly, but in a more detailed way, to what happens as regards nutritional claims (https://ec.europa.eu/food/safety/labelling_nutrition/claims/nutrition_claims_en)

lists "without the submission of data designated as proprietary by the prior applicant".

Recital 32 clarifies the rationale of these provisions, i.e. stimulating research and development in the industry by protecting the underlying investment. The 5-year time limitation is a necessary constraint to avoid repeated trials (as with GM food), but also to "facilitate access to claims by small and medium-sized enterprises (SMEs), which rarely have the financial capacity to carry out research activities". However, this protection for the investment has been considered limited when scholars compared them to the combination of data protection and confidentiality rules that is typical of other sectoral legislations, such as food improvement agents (additives, enzymes, flavourings) (Sachs, 2016, p.436).

3.2.3 Regulation 2015/2283 on Novel Foods

Regulation 2015/2283 ("Novel Foods Regulation")[137] disciplines the placement on the market of foods that have not been consumed in the EU since a precise day (15 May 1997) and that belong to one of the categories listed in Article 3(2). The placement on the market of novel foods follows an authorisation not dissimilar from the ones discussed above: the applicant has to demonstrate that the novel food does not pose a safety risk to human health by submitting scientific evidence within its application (Art. 10(2)(e)) and, following EFSA's scientific opinion, the Commission takes the decision to include the novel food at stake in the list of authorised products[138].

Alternatively, when an applicant is willing to place a traditional food from a third country (Art. 3(2)(c)), it may follow the procedure set up by Section II of the Novel Foods Regulation. Instead of documenting the safety of the novel food, applicants shall provide "documented data demonstrating the history of safe food use in a third country" (Art. 14(e)). EFSA has then to verify:

- the history of safe food use in a third country is substantiated by reliable data submitted by the applicant (Art. 17(2)(a))

[137] Regulation (EU) 2015/2283 of the European Parliament and of the Council of 25 November 2015 on novel foods, amending Regulation (EU) No 1169/2011 of the European Parliament and of the Council and repealing Regulation (EC) No 258/97 of the European Parliament and of the Council and Commission Regulation (EC) No 1852/2001 [2015] OJ L327/1

[138] Annex of the Commission Implementing Regulation (EU) 2017/2470 of 20 December 2017 establishing the Union list of novel foods in accordance with Regulation (EU) 2015/2283 of the European Parliament and of the Council on novel foods [2017] OJ L 351/72

- whether the composition of the food and its use do not pose risk to human health (Art. 17(2)(c))

- whether a replacement of other foods would be disadvantageous for the consumers (Art. 17(2)(c))

Implementing regulations from the Commission reflect the different data requirements for the applicants. According to the wording of the Novel Foods Regulation, the rationale underlying this differentiation is the need of simplifying the burdens for the applicants, thus encouraging the marketing of traditional foods from third countries whose safety has been demonstrated by the experience of continuous use for at least 15 years (Recital 15).

Article 5 of the Commission Implementing Regulation 2017/2469 on novel foods only[139] provides for a detailed list of scientific data required. They include :

- a copy of the documentation on the procedure and strategy followed when gathering the data (Art. 5(3));

- a description of the safety evaluation strategy and the corresponding toxicological testing strategy, including the rationale underlying the exclusion of certain studies (Art. 5(4));

- on request, raw data of single studies, published and unpublished, undertaken by the applicant, or on their behalf, to support their application. This requirement also includes data used to generate the conclusions of the individual studies and results of examinations (Art. 5(5)), and

- data on the effects of the novel food on groups other than the particular one for which consumption of the novel food is also intended (Art. 5(6)).

Conversely, Commission Implementing Regulation 2017/2468 on traditional foods from third countries[140] eases the burden of the applicants, which have to provide, together their conclusions:

- a dossier showing a history of safe use of the traditional food from third coun-

[139] Commission Implementing Regulation (EU) 2017/2469 (EU) of 20 December 2017 laying down administrative and scientific requirements for applications referred to in Article 10 of Regulation (EU) 2015/2283 of the European Parliament and of the Council on novel foods

[140] Commission Implementing Regulation (EU) 2017/2468 of 20 December 2017 laying down administrative and scientific requirements concerning traditional foods from third countries in accordance with Regulation (EU) 2015/2283 of the European Parliament and of the Council on novel foods [2017] OJ L 351/55

try (Art. 6(1));

- a copy of the documentation on the procedure followed when gathering the data (Art. 6(2)), and
- a description of the safety evaluation strategy and the rationale underlying the exclusion of certain studies (Art. 6(3))

Information provided by the applicants may be subject to confidentiality measures (if requested) if the disclosure may harm their competitive position. In the current wording of Article 23 of the Novel Foods Regulation, confidentiality requests cannot apply on the summary of the studies submitted by an applicant (Art. 23(4)(d)), the results of the studies carried out to demonstrate the safety of the food (Art. 23(4)(e)) and, where appropriate, the analysis method(s) (Art. 23(4)(f)). As with other pieces of legislation analysed above, "verifiable justification" shall be given (Art. 23(1)) to support the confidentiality claim. Moreover, the protection of human health may prevail on confidentiality measures, when needed (Art. 23(6)). Finally, confidentiality measures does not hamper information sharing between the Commission, the reporting Member State and EFSA (Art. 23(7)).

The Transparency Regulation has replaced the text of Article 23 by harmonising the confidentiality claim procedure to the one described in Articles 38 to 39f of the amended GFLR (new Art. 23(3)) and enlarging the scope of confidentiality requests with respect to manufacturing process, except for information which is relevant for risk assessment (new Art. 23(4)). However, the elements previously displayed in Article 23 which cannot be subject to confidentiality request are no longer present in the newly adopted version. Instead, the provision under new Article 23(2)[141] is relatively controversial for at least two reasons. First, while confidentiality requests could now extend to all the elements submitted in the context of an application, the amended GFLR could prevail by means of the new Article 23(3), thus limiting the remit of claims to elements listed in Article 39 of the GFLR notwithstanding the *lex specialis* principle. Second, in the current wording of the Novel Foods Regulation, applicants shall substantiate their request by providing information on how the disclosure of data "may harm their competitive position" (Art. 23(1)). In the absence of any reference to competitive power and if the GFLR prevail, applicants shall now demonstrate "how making public the information concerned significantly harms the interests", which are considerably broader that the competitive position, as it might also include, for instance, intellectual property rights or brand reputation.

[141] New Art. 23(2): [t]he applicant may submit a request to treat certain parts of the information submitted under this Regulation as confidential, accompanied by verifiable justification, upon submission of the application

Data protection measures also apply to novel foods[142]. Article 26 of Regulation 2015/2283 states that "newly developed scientific evidence or scientific data supporting the application shall not be used for the benefit of a subsequent application during a period of five years" from the date of the first authorisation (Art. 26(1)), unless the initial and the subsequent applicant find an agreement (Art. 26(3)). The rationale underlying this protection is the protection of stimulating research and development in the industry (Recital 30).

Three conditions have to be met to obtain protection benefits:

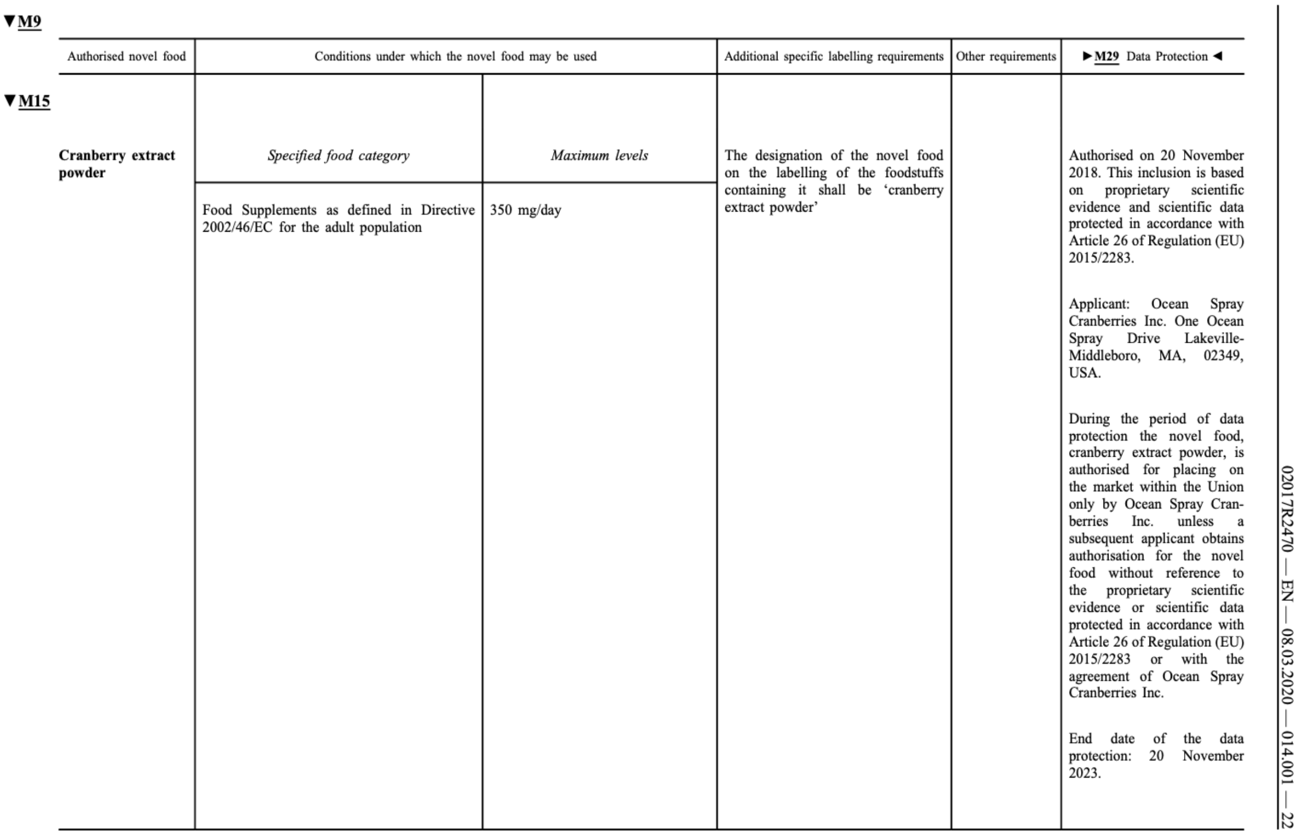
- The initial applicant has designated newly developed scientific evidence or scientific data as proprietary;

- The initial applicant has an exclusive right to reference to the newly developed scientific evidence or scientific data; and

- The risk assessment of the novel foods would not have been possible without the submission of the proprietary scientific evidence/data

The novel food list shall also report that the inclusion of proprietary data (Art. 27(b)), mention the fact that subsequent applicants cannot rely on the data of the first applicant (Art. 27(c)) and the expiration date of the data protection (Art. 27(d)). The following figure shows an entry on the novel foods list - Cranberry extract powder (EFSA, 2017) - containing data protection indications.

[142] Instead, they not do apply to traditional foods from third countries (Art. 26(3)) since the burden to prove safety is considerably lower, as noted above



▼M9

▼M15

Authorised novel food	Conditions under which the novel food may be used		Additional specific labelling requirements	Other requirements	►M29 Data Protection ◄
Cranberry extract powder	*Specified food category*	*Maximum levels*	The designation of the novel food on the labelling of the foodstuffs containing it shall be 'cranberry extract powder'		Authorised on 20 November 2018. This inclusion is based on proprietary scientific evidence and scientific data protected in accordance with Article 26 of Regulation (EU) 2015/2283. Applicant: Ocean Spray Cranberries Inc. One Ocean Spray Drive Lakeville-Middleboro, MA, 02349, USA. During the period of data protection the novel food, cranberry extract powder, is authorised for placing on the market within the Union only by Ocean Spray Cranberries Inc. unless a subsequent applicant obtains authorisation for the novel food without reference to the proprietary scientific evidence or scientific data protected in accordance with Article 26 of Regulation (EU) 2015/2283 or with the agreement of Ocean Spray Cranberries Inc. End date of the data protection: 20 November 2023.
	Food Supplements as defined in Directive 2002/46/EC for the adult population	350 mg/day			

02017R2470 — EN — 08.03.2020 — 014.001 — 22

Figure 3.2: Novel Food list item (Cranberry extract powder) extracted from Annex I of Commission Implementing Regulation 2017/2470. Data protection measures are reported on the last column

3.3 Reviewed case-law of the Court of Justice on transparency and confidentiality of private information

Another significant contribution to the debate surrounding transparency measures *vis-à-vis* confidentiality and data protection is the one made by the jurisprudence of the Court of Justice of the European Union (CJEU). Over the last years, its decisions have progressively adopted a "more transparency" approach by confining the remit of confidentiality measures due to an overriding public interest in the disclosure of data. This section aims to reconstruct the judicial reasoning of the Court, the goals of transparency in its words, and how the balance of public and private interests has been struck in practice. Consistently with the scope of this study, our focus will be on cases that explicitly confront with data-related issues in the food safety risk assessment domain[143].

This section refers to a specific sectoral legislation, i.e. the legal framework for the application to place Plant Protection Products (PPPs, usually referred to as "pesticides") in the EU market. The applicable legislation consists of Regulation 1107/2009[144], Commission Regulation 546/2011[145] and Commission Regulation 284/2013[146] which mandate the submission of data (Art. 8 of Regulation 1107/2009) by the applicant and a review by EFSA (Art. 12 of Regulation 1107/2009) following a preliminary assessment of the Member State to which the application was first referred. The same applies in the case of renewal. Transparency Regulation has harmonised the handling of confidentiality claims regarding PPPs to the procedure set out in the GFLR.

Similarly to what has been noted in §3.2.1 regarding the use of GM food and feed, this legal framework is further enriched by the applicability of the Aarhus Regulation, which requires that EU bodies make available environmental information upon request based on Regulation 1049/2001 and following an assessment of possible derogations while bearing in mind their restrictive interpretation. As discussed above, exceptions may include the protection of legitimate commercial interests of

[143] Nevertheless, some other cases might be of interest for contextualising the ones discussed in the next sections. *Inter alia*, Case T-70/99 *Alpharma Inc. v Council of the European Union* ECLI:EU:T:2002:210 [2002] ECR-II-03495 frames the scope of risk assessment and its relationship with risk management in light of the precautionary principle ("Notwithstanding the existing scientific uncertainty, the scientific risk assessment must enable the competent public authority to ascertain, on the basis of the best available scientific data and the most recent results of international research, whether matters have gone beyond the level of risk that it deems acceptable for society") [para 175] (Rusconi, 2016, p.457). An other case settled on the same day - Case T-13/99 *Pfizer Animal Health SA/NV v Council of the European Union* EU:T:2002:209 [2002] ECR-II-03305 - clarified that "scientific advice on matters relating to consumer health must, in the interests of consumers and industry, be based on the principles of excellence, independence and transparency". This wording is particularly significant due to the concomitant institution of EFSA, which was established a few months before the General Court's decision. The wording of the General Court in this case has been interpreted as a remark to provide rigorous standards in the definition of prerequisites of decision-making (J. Peel, 2012). A similar approach has been taken in a later case - C-79/09 *Gowan Comércio Internacional e Serviços Lda v. Ministero della Salute* EU:C:2010:803 [2010] ECR I-13533 annotated by Alemanno (Alemanno, 2011)

[144] Regulation 1107/2009 of the European Parliament and of the Council of 21 October 2009 concerning the placing of plant protection products on the market and repealing Council Directives 79/117/EEC and 91/414/EEC [2009] OJ L 309/2009

[145] Commission Regulation 546/2011 of 10 June 2011 implementing Regulation (EC) No 1107/2009 of the European Parliament and of the Council as regards uniform principles for evaluation and authorisation of plant protection products [2011] OJ L 155/127

[146] Commission Regulation 284/2013 of 1 March 2013 setting out the data requirements for plant protection products, in accordance with Regulation (EC) No 1107/2009 of the European Parliament and of the Council concerning the placing of plant protection products on the market [2013] OJ L 93/85

a third party, including intellectual property. However, Aarhus Regulation states the prevalence of the public interest in the disclosure.

As it will be shown, together with conclusions applicable to each controversy, this analysis identifies an interpretative mechanism put in place by the CJEU courts, i.e. a principle-based approach that is used to identify the rationale of reactive and proactive measures of data publication or access. Once clarified their scopes, these principles serve to identify criteria used to settle the dispute, usually by declaring the prevalence of the public interest in the disclosure. This leaves open questions regarding the possibility to extend the information to be made available (reactively or proactively) to other informational components (e.g. computer programmes and operational data) following the same approach and the same criteria adopted by the CJEU.

3.3.1 *Greenpeace and PAN Europe* on the concept of environmental information and on the balance of public and commercial interests

In 2013, a remarkable case (Moules, 2017) discussed the reactive disclosure of documents by the Commission when environmental information is at stake. In the controversy - *Greenpeace Nederland and Pesticide Action Network Europe v Commission*[147] - the General Court had to confront with the interpretation of what constitutes information relating to emissions into the environment. Defendants requested access to documents and data on the composition of a glyphosate-based pesticide [paras 2, 17]. Although EFSA was not directly involved in these cases, this controversy is worth of mention due to the discussion regarding the public disclosure of commercial information that originated from this case (Korkea-Aho and Leino, 2017, p.1080). It is also significant under two profiles: on the one hand, the decision clarifies the scope of "information *related* (emphasis added) to emissions into the environment" for the purposes of Aarhus Regulation, which apply to subject matters under the competences of EFSA; on the other hand, it points out whether the balance between public interest in the disclosure and the commercial interests in protecting valuable information should be done in abstract or by looking at concrete factors.

Applicants of the case requested access to environmental information on certain PPPs held by the Commission and transmitted by the German Government. The Commission partially rejected the request by claiming that over a specific volume,

[147] Case T-545/11 *Stichting Greenpeace Nederland and PAN Europe v Commission* EU:T:2013:523

containing a "complete list of all tests", the German authority had refused to provide access and the Commission was in turn obliged to act in compliance with its decision. German authorities had previously declared that they did not consider to be an overriding public interest for the disclosure of the concerned document[148] and the information contained were not pertaining to emissions into the environment [para 7]. The Commission opted to protect intellectual property rights over the public interest in the disclosure of data, deeming the previous publications adequate to ensure transparency [paras 9-11].

In the judgement, the General Court first restated that one of the goals of Regulation 1049/2001 is to favour open decisions to strengthen democracy [para. 27], consistently with its previous case-law. In *Turco*[149] the ECJ had observed, when referring to the goals of Regulation 1049/2001, that: "[o]penness in that respect contributes to strengthening democracy by allowing citizens to scrutinize all the information which has formed the basis of a legislative act. The possibility for citizens to find out the considerations underpinning legislative action is a precondition for the effective exercise of their democratic rights" [paras 41-43, 59-61].

Second, when confronting with the exceptions to the disclosure for reasons of protecting private interests, the General Court observed that "since they derogate from the principle of the widest possible public access to documents, those exceptions must be interpreted and applied strictly" [para 32] and in line with TRIPS (Trade Related Aspects of Intellectual Property Rights) Agreement, when possible[150]. Therefore, the Court concluded that exceptions to the general rule of disclosure, including the intellectual property, must be interpreted and applied strictly to not to frustrate the goals of Regulation 1049/2001 [para 50].

Third, the General Court remarked that Recital 15 of the Aarhus Regulation calls for a restrictive interpretation of the grounds of refusal of public access. When assessing the request, authorities shall consider two factors, namely the "public interest the disclosure" and the relationship between the information and emissions into the environment [paras 52-53]. As regards the former, it is unclear whether

[148] In particular, it has been argued that, by giving access to the documents at stake, other competitors would have been able to to copy the production processes, thus leaving commercial interests and intellectual property rights unprotected (Bazylińska-Nagler, 2017)

[149] Casae C-39/05 *Sweden and Turco v Council* [2008] ECR-I-04723

[150] While TRIPS agreement are outside the scope of this thesis, it has to be remarked that the Court also discussed the relationship between EU provisions and the TRIPS agreement, which is part of the internal legal framework of the Union. It stated that "[w]here there are European Union rules in a sphere concerned by the TRIPS Agreement, European Union law will apply, which will mean that it is necessary, as far as possible, to adopt an interpretation in keeping with the TRIPS Agreement, although no direct effect may be given to the provision of that agreement at issue" [paras 45-46]. For an extensive discussion on TRIPS and environmental information in this judgement, see the case note by von Holleben (Holleben, 2013, sec. II(2))

the public interest should be evaluated *in abstracto* or *in concreto* terms[151]. Regarding the latter, the Court interpreted such relationship as a "sufficiently direct link" [paras 53, 57], in a manner that the concept of "information relating to emissions into the environment" also includes the contents of the dossier at stake [paras 60 - 61, 66]. On this ground, the General Court annulled the decision at issue by the Commission, insofar as it refused access to those parts of the dossier including information on "emissions into the environment" as interpreted above. One commentator (Holleben, 2013, p. 575) has criticised the adoption of such criterion by claiming its extensive broadness, up to the point to run "the risk of classifying the entire use of chemicals as emission".

In the appeal[152], the ECJ accepted the premise of interpreting exceptions to the divulgation of information related to emissions into the environment restrictively [para 50]. However, while adopting the same principle-based approach of the first instance, it rejected the "sufficiently direct link" criterion and adopted a new standard, namely that the concept of "emissions into the environment" covers "information on current and foreseeable emissions", whereas it does not include "purely hypothetical emissions" (Moules, 2017) [para 73-75]. One commentator (Bazylińska-Nagler, 2017) has noted that other formulae ("information which relates to emissions" and "information with a sufficiently direct link to emissions") contributed to the overall vagueness of the terminology used by the ECJ.

The teleological interpretation of the dissemination obligation is particularly significant. The ECJ stated that the concept access to environmental information "must be understood to include, *inter alia*, data that will allow the public to know what is actually released into the environment", including foreseeable effects [para 79]. The list of information to be made available - "information concerning the nature, composition, quantity, date and place of the actual or current and foreseeable emissions, under such conditions, from that product or substance" - that follows this statement is a consequence of this rationale. Moreover, such dissemination is needed a) to include citizens in decision-making processes, the accountability of decision-makers and the public awareness of environmental matters [para 80], and b) for reasons of consistency with the general aims of Regulation 1049/2001, i.e. "the balance which

[151] For instance, whether or not the commercial/non-governmental nature or the purposes of the requester should be kept into account or the Commission should evaluate them broadly. One commentator (Holleben, 2013, p. 571) has noted that the General Court found an irrebuttable statutory presumption in the conjunction between Art. 4(2) of Regulation and the Aarhus Regulation that prevents any further balancing of conflict of rights by making the public interest in the disclosure prevailing *iuris et de iure* without the need of assessing the peculiarities of the request

[152] Case C-673/13 P *Commission v Stichting Greenpeace Nederland and PAN* Europe [2016] ECLI:EU:C:2016:889. Noteworthily, the case saw written observations by CropLife International, National Association of Manufacturers of the United States of America, America Chemistry Council Inc., European Crop Care Association, European Chemical Industry Council, and Association européenne pour la protection des cultures in support of the Commission

the EU legislature intended to maintain between the objective of transparency and the protection of those interests" [para 81]. On this basis, the ECJ set aside the judgment of the General Court and referred it back.

As noted by a commentator (Moules, 2017), the line between "foreseeable" and "purely hypothetical" emissions may sound unclear. On the same day, the Court delivered another ruling - *Bayer CropScience*[153] - in which it clarified that information on "current and foreseeable emissions" consists of "data concerning the medium to long-term consequences" of emissions and studies on the measurement of the substance's drift when realistic conditions - yet, "most unfavourable" [para 91] - but it does not cover simulations in which normal or realistic conditions are not met due to "significantly" higher doses [para 90].

Finally, the case came to its conclusion in 2018[154]. The General Court accepted the "information on current and foreseeable emissions" criterion [para 57-58] and concluded that the Commission "did not commit an error of assessment in considering that the document at issue does not contain information relating to emissions into the environment" [para 91], contrary to what stated in the previous judgement.

Moreover, the General Court also provided answers for the question pertaining whether the evaluation of the balance of public and commercial interests should be carried out in abstract or practical terms. The General Court opted for the latter approach by stating that "it must be shown that the documents at issue contain elements which may, if disclosed, seriously undermine the commercial interests of a legal person" [para 110]. In the case at stake, the General Court did not confirm its previous decision and approved the balance of interests carried out by the Commission [paras 111-112].

In summary, the controversy provided answers for some interpretative doubts regarding the nature of "environmental information" in the case of PPPs and how the balance between public and private interests regarding this information should be assessed. As regards the first issue, the information-types at stake are not relevant for our discussion. Instead, the criterion to assess whether or not the information should be made available is of particular interest. Two criteria, namely the "sufficiently direct link" and "information on current and foreseeable emissions" were adopted, with the latter prevailing in the end. Commentators from ClientEarth (Buonsante and Friel, 2017, p. 457) noted that the "foreseeable emission" criterion would hinder the possibility to access studies where higher doses are tested to verify acute and long-term exposure and proposed a broader interpretation that shall

[153] Case C-442/14 *Bayer CropScience SA-NV and Stichting De Bijenstichting v College voor de toelating van gewasbeschermingsmiddelen en biociden* [2016] ECLI:EU:C:2016:890

[154] Case T-545/11 RENV *Stichting Greenpeace Nederland and PAN Europe v Commission* ECLI:EU:T:2018:817

include all the documents used to draw conclusions about current and foreseeable emissions.

In light of our data-centric analysis, this controversy and the "foreseeable emission" vs "purely hypothetical emission" debate is particular significant. Considering the higher relevance of data analysis discussed in the Chapter 2, not only are raw data becoming as relevant as documents, but also advanced analysis techniques increasingly contribute to the amount of studies that are carried out to assess the exposure to regulated products with potential impact on the environment, including pesticides and GM food and feed. This may entail that algorithms and operational data about their accuracy (e.g. precision, recall, confidence scores, etc.) might fall under the remit of environmental information as far as they contribute to the general foreseeability of the emissions.

A positive answer to this hypothetical will be argued by relying on the teleological interpretation used by the ECJ to define the "current and foreseeable emissions" criterion. The ECJ stated that the overall goals of environmental-related provisions of Regulation 1049/2001 - as interpreted in light of the Aarhus Regulation - are the involvement of citizens in decision-making processes, the accountability of decision-makers and the promotion of public awareness of environmental matters. For these reasons, certain data were listed among the ones to be reactively published. This interpretation entails that any reactive disclosure of data must keep into account "data that will allow the public to know what is actually released into the environment" [ECJ judgement, para 79] insofar they allow a greater forseeability of emissions. Algorithms and operational data contribute to the explanation of scientific evidence used in support of applications and allow for the cross-validation of forecasts and other predictions[155].

3.3.2 *Tweedale* and *Hautala* on the overriding public interest on the disclosure of confidential dossiers

On 7 March 2019, the General Court delivered two cases, *Tweedale*[156] and *Hautala*[157], which directly concerned EFSA and its decisions.

Tweedale case pertains to the access to documents related to Glyphosate. In 2014, Anthony Tweedale, a consultant on environmental matters, requested EFSA to ac-

[155] This position will be further discussed in §5.2.4 on Explainability

[156] Case T-716/14, *Anthony C Tweedale v European Food Safety Authority* [2019] ECLI:EU:T:2019:141

[157] Case T-329/17, *Heidi Hautala and Others v European Food Safety Authority* [2019] ECLI:EU:T:2019:142

cess documents related to two "key studies used in order to set Glyphosate's acceptable daily intake (ADI)" [para 9], pursuant to Regulation 1049/2001. EFSA had these studies in its possession pending Glyphosate assessment. The Authority refused the access due to the exception related the protection of commercial interests (Art. 4(2) of Regulation 1049/2001).

According to EFSA, such protection was due to the confidential status that was granted in the application procedure [para 8]. EFSA also considered that the proactive publication of scientific information relating to the safety of Glyphosate was "manifestly and fully satisfied" by the data made available on its website [para 12]. In 2017, following several rounds of discussion, EFSA decided to give access to raw data and findings of the two "key studies" while also claiming that confidentiality status did not apply to that information [para 18-20]. However, the Authority gave only limited access and kept confidential some administrative and manufacturing information, as well as information related to the protocols followed by the study owners [para 21]. EFSA acted on the basis of a "balance of interests" analysis and concluded that no overriding public interest could have been found in the non-disclosed information. It concluded that "raw data and findings were sufficient to examine carefully the evaluation of the results of the requested studies" [para 23]. The case stayed pending until the final judgements of *Commission v PAN Europe* and *Bayer CropScience* [para 27] and resumed after their final delivery [para 31].

Applicant raised a total of six pleas, which could be summarised in two broad categories: on the one hand, that EFSA had misclassified the non-disclosed information in both decisions (first and fifth claims); on the other hand, that EFSA had let the private interest in keeping data confidential prevail over the public one in disclosure while failing to provide sufficient justifications to keep the undisclosed data away from public eyes (second, third, fourth, and sixth claim).

Hautala case has a similar factual background. In 2016, Ms Heidi Hautala and other four MEPs requested access to glyphosate-related scientific studies held by EFSA, this time by justifying their request by highlighting the IARC- EFSA controversy discussed in §2.4.2. As in *Tweedale*, EFSA granted access to a large *corpus* of unpublished studies, including raw data and findings, while keeping material, experimental conditions and methods secret, likewise results and discussions (Morvillo, 2019). As with *Tweedale*, EFSA relied on a twofold rationale: on the one hand, the disclosure would have harmed the commercial interest of the the concerned company [paras 22-23]; on the other hand, the requested studies did not fall within the remit of "environmental information" to be reactively disclosed [para 24]. Pleas made by applicants were substantially the same as the ones in *Tweedale* (Morvillo, 2019).

As regards the scrutiny of the balance of public and private interests, the Court consolidated its narrow interpretation of the confidentiality exceptions with respect to general principle of transparency. The Court remarked that, in Regulation 1049/2001, "openness enables the EU institutions to have greater legitimacy and to be more effective and more accountable to EU citizens in a democratic system and that, by allowing divergences between various points of view to be openly debated, it also contributes to increasing those citizens' confidence in those institutions" [*Tweedale*, para 75; *Hautala*, para 60]. Such teleological interpretation of the rationale underlying Regulation 1049/2001 is not entirely new, since the Court had already introduced it in *ClientEarth v Commission*[158] [para 75].

With regards to the nature of approval dossiers of PPS submitted by applicants for authorisation, they were qualified as "environmental information" by the Court. The rationale was the same used in *Stichting Greenpeace Nederland and PAN Europe v Commission* after the previous judgement by the CJEU. [*Tweedale*, paras 80-88, *Hautala* paras 84-90]. One commentator (Morvillo, 2019) observed how the notion of "environmental information" has been interpreted in light of the balance struck between openness and commercial interest when controversial types of information are at stake. While we agree with this note, some additional remarks are necessary.

The reasoning of the Court can be also read as a principle-based approach: first, the rationale underlying transparency and openness of risk assessors and managers is defined; then, a criterion of inclusion of information-types is identified; finally, individual information-types are included or excluded on the basis of this rationale. Such teleological interpretation has been provided by means of "guidelines" [*Tweedale* para 93, *Hautala*, para 100] issued by the Court itself and addressed to EFSA and the Commission. If this interpretation of Court's reasoning is correct, the question posed by one commentator (Morvillo, 2019) regarding the generalisability of Court's findings in *Tweedale* and *Hautala* can be answered by the extent to which the rationales of transparency and openness are capable of setting inclusive criteria and, in turn, information-types: the broader the scope of the two principles, the more data-types will be included.

To this extent, when comparing *Tweedale* and *Hautala* with their predecessor (*Commission v Stichting Greenpeace Nederland and PAN Europe*), it can be noted that the Court adopted a broader definition of openness. In the former two cases, openness is understood as broader principle that aims to promote democracy, accountability and trust; in the latter, the CJEU seems to not have discussed openness in general, rather narrowing its focus on proactive transparency measures in environ-

[158] Case C-57/16 P *ClientEarth v Commission* [2018] ECLI:EU:C:2018:660. In this case, the conflicting interests were represented by the public interest in disclosure of environmental impact assessment reports held by the Commission and the interest of the Commission itself in keeping a document secret during an ongoing decision-making process, a possibility granted by the exceptions provided by Art. 4(3) of Regulation 1049/2001. The former prevailed to prevent opaque external pressures over decision-makers (Berthier, 2016)

mental matters[159]. Despite the different scope, the two approaches converge to one single criterion ("current and foreseeable emissions") that allows the inclusion of different information-types.

As this dissertation analyses the general balance of public and commercial interests also in the context of reactive transparency, it is then necessary to "learn the lesson" from the mentioned case-law on proactive measures and, in particular, the principle-based approach, while attempting to adapt it to the technical context and the amended legal framework of reactive transparency measures. Raw data, algorithms/source codes and operational data would certainly be needed in order to scrutinise the impact of regulated products on the environment, including emissions.

If this interpretation is correct, it could also solve the gap left open by commentators (Korkea-Aho and Leino, 2017, p.1082) when posing the doubt regarding the problem of "irrelevant" data, whose obligation to disclose is questioned. It is argued that mandatory disclosure "only relates to relevant data that can be extracted from the source of information and separated from other information contained in that source" (Korkea-Aho and Leino, 2017, p.1082). Insofar such information (raw data, algorithms/source codes and operational data) is essential to foresee adverse health effects, an overriding public interest should be deemed to exist[160].

It is incredibly hard to tell whether and when a similar case - in which environmental information are inferred from confidential data using probabilistic models and the access request includes operational data - would be brought before European courts. If the ongoing datafication continues, it is likely that Courts will be forced to confront with these issues. To reason about to this eventuality, it is necessary to focus on openness and transparency also in the context of ongoing datafication trends.

[159] *Commission v Stichting Greenpeace Nederland and PAN Europe*, para 79: [i]t is apparent, in essence, *from recital 2 of Regulation No 1367/2006* (emphasis added) that the purpose of access to environmental information provided by that regulation is, inter alia, to promote more effective public participation in the decision-making process, thereby increasing, on the part of the competent bodies, the accountability of decision-making and contributing to public awareness and support for the decisions taken.

[160] This interpretation has also a strong epistemic relevance as the "essentiality" of this information is also needed to prevent "black box" problems in the machine learning algorithms deployed in this context. This dimension will be covered in §5.2.4 on Explainability

3.3.3 *Arysta LifeScience Netherlands BV v EFSA* on confidentiality claims decisions

Finally, a case - *Arysta LifeScience Netherlands BV v EFSA*[161] - is discussed to cast light on the judicial review of the decisions regarding the confidential treatment of commercially sensitive information by EFSA when the public interests to access information has to be balanced with legitimate business interests.

In 2013, the Commission initiated the peer review of the active substance diflubenzuron, an insecticide used on apples, pears and mushrooms, and other crops [paras 25, 30]. In 2015, EFSA delivered its opinion and raised *a priori* concerns regarding the potential exposure to the substance named "PCA (4-chloroaniline)" and "its potential toxicological relevance for consumers, workers and residents or bystanders", also due to lack of data [paras 35-38]. On its own initiative, EFSA decided to publish its conclusions on its website. Before the publication, EFSA asked the applicant to identify possible confidential information in the conclusion, but eventually granted confidentiality status only to names of the authors of studies and reports, whereas it rejected the request grounded on the potential harm to applicant's commercial interests [para 39-40]. This choice was justified by the paucity of possible harm to applicant's image when confronted to its obligation to publish information likely to affect public health [para 41].

By means of five pleas, *inter alia* the applicant contested EFSA's decision to not to grant confidential treatment over the information for which it was requested. In particular, the applicant claimed that the scientifically incorrect assessment in question undermined its commercial interests and its reputation [para 105]. With this regard, EFSA noted that its conclusions were to be made available to the public for the protection of public health [para 106].

The General Court dismissed the action. While doing so, it provided a series of interpretative guidelines for the handling of confidentiality claims. First, the Court confirmed that "confidential treatment of information [...] is the exception, whereas public access to that information is the rule", even when applicant's interest is legitimate [para 99]. Article 63 of Regulation No 1107/2009 contains an "open list" of information that might be subject to confidentiality claims, as long as the entity supporting them provides "verifiable evidence showing in a concrete manner that the disclosure of that information might undermine his commercial interests" [para 108]. However, such possible harm cannot derive from the potential wrongfulness of the scientific conclusions [para 110].

[161] Case T-725/15 *Arysta LifeScience Netherlands BV, formerly Chemtura Netherlands BV, v EFSA* [2018] ECLI:EU:T:2018:977

The Court also recalled that Article 63 of Regulation 1107/2009 promotes a balance between the transparency of review process and the protection of business secrets. To define what information falls within the remit of the notion of "business secrets", the Court recalls the three criteria already discussed in §3.1.2, i.e. the secrecy of information, the harmfulness of data publication and the objective worthiness of the interests underlying the non-disclosure of data. Such interests have to be weighted against the public interest that EU institutions' activity - including EFSA's risk assessment - are carried out "as openly as possible" (Jaeger, 2019).

Applicant's claim was rejected do to its failure to provide "verifiable evidence" of the alleged threat to its business interests [para 130]. The Court also affirmed *ad abundantiam* the goodness of EFSA's decision on disclosing information on "foreseeable health effects of the active substance at issue", also noting a settled jurisprudence that justifies the precedence of human health over economic considerations [paras 131-134].

General Court's final remark is the *trait d'union* between the present case and the other discussed in the previous sections. As with the cases of "reactive" transparency, the Court adopted a principle-based approach - hence, first the identification of the rationale underlying transparency and openness, then the definition of a criterion to include information-types, and finally the selection of information-types - when evaluating the decision of an EU institution in the case of "proactive" transparency measures. Differences and similarities, however, have to be noted.

On the one hand, the rationale underlying transparency in *Arysta* diverges from the one of the previous cases: data disclosure is justified by the protection of human health rather than the promotion of awareness and transparency in decision-making processes. One could argue that such an explanation is mainly due to the sectoral legislation at stake. However, this would be in conflict with the *obiter dicta* regarding openness from other cases, in which the Court had to confront with sectoral legislations as in *Arysta*. A more correct interpretation seems the one which suggests that, in *Arysta*, there was no risk-related "decision"[162] involved, since the whole controversy took place in the assessment stages, which are usually prior to the actual "decisions" taken by the risk managers, as it was in the other cases. Therefore, a general remark could suggest that the goals of transparency identified in the previous cases could not apply to the assessment scenario at stake in *Arysta*.

On the other hand, while the principle of transparency was grounded on a different rationale (protection of public health *vìs-à-vìs* transparency of risk management

[162] In the case at stake, the only decisions concerned are the ones taken by EFSA when opting for the publication of allegedly confidential information. This decision, however, occurred within risk assessment and should not be deemed to have managerial implications, i.e. the authorisation/denial to place the production on the market

decisions), the identified criterion for solving the controversy is substantially the same, i.e. the foreseeability of health-related effects of regulated products. While in the previous cases such criterion was meant to be the gateway to include information among the ones to be published (*in concreto*), in *Arysta* it has been used as a justification of the balance struck between the public interest in proactive disclosure and commercial interests of undertakings by the European legislator (thus, *in abstracto*).

These findings leave open the question regarding how to interpret the principle of transparency in our domain. If, in spite of different underlying rationales, transparency is understood as a way to allow the forseeability of health-related concerns by citizens both in reactive and proactive disclosure measures, this implies that, in light of the current datafication process, other informational components can be subsumed within the information needed for such foreseeability, not only in the context of reactive transparency measures - as argued above - but also for proactive transparency provisions. Forseeability seems also to be appropriate for dealing with risk assessment and risk communication: even though we noted that the rationale underlying transparency is different among the case law, its alignment in a "transparency-as-foreseeability" interpretation seems consistent across all areas of risk analysis.

In conclusion, our analysis suggests that "transparency-as-foreseeability" is a viable way to read the case-law of the CJEU in cases regarding the disclosure of environmental information. Such interpretation is mainly due to a principle-based approach that, following the identification of a rationale for transparency and openness, identifies a criterion to include certain information types (*rebus sic stantibus*, forseeability) and proceeds with the inclusion of specific data-types. Following *Tweedale* and *Hautala*, the "more transparency" approach proposed by the Legislator inb the drafting of the 2019 Transparency Regulation can also be found in the recent jurisprudence of the CJEU, not only in the field of reactive transparency measures, but also when EFSA acts to divulge data or assesses confidentiality claims.

Will such convergence align with the new Transparency Regulation? I would cautiously suggest a positive answer. The overall rationale of the Regulation is, in essence, aligned with abstracts goals of ensuring trust in decision-makers by allowing scrutiny of their activities. However, different interpretations of the goals of transparency and openness, as well as an ambiguous use of these terms, might hinder the goals of promoting a unified approach towards "more transparency". Moreover, more speculative questions are left unanswered, in particular with regards to a) the changing nature of data ownership in this domain following the novel approach of the CJEU, and b) the relationship between environmental information and algorithms in light of this case law.

3.4 Trust, data ownership and future legal challenges

This final section aims to cast light on a several issues related both to the amendments made to the GFLR and to the case law of the CJEU. This analysis is not limited to evidence from the academic literature on certain issues that might be of interest in light of the principle-based discourse of the next Chapter, but it also includes contributions related to broader topics discussed by policy-makers.

Following a tentative interpretation of data ownership in this domain, this section ends with three sets of conclusions: first, a concise commentary on the concepts of transparency and openness in the amended food safety legislation is provided; then, the implications of these preliminary conclusions as regards the question of data ownership are discussed; finally, future legal challenges that have been left unanswered by the current framework are identified to bridge the gap with the next Chapter.

3.4.1 An ownership-based approach to openness and transparency in the amended Food Safety legislation

Considering the legislative amendments and the reading of CJEU case law, it seems possible that the transparency principle has become a "one-fits-all" solution for several issues that affect food safety legislation, not least the lack of trust in the system. Both in the newly amended legislation and in the reasoning of the CJEU, it is assumed that trust in food assessors and mangers will increase by providing access to individuals, being they citizens, MEPs or independent scientists to the data held by the competent authorities. This dissertation does not aim to verify the validity of this statement. Instead, it will look at the implications of this increased scope of transparency on trust from an ownership-based viewpoint.

In light of the legal framework analysed so far, the principle of transparency is critically multi-faceted when it comes to its goals. Our analyses underlined that this principle is invoked to foster trust in food safety authorities, promote democracy, make EU food safety institutions accountable, protect human health, allow the public oversight of decision-making processes, and so on. While some of these goals are inextricably linked, other seems too far to be included with the operational remit of one single principle[163].

[163] Nothing would prevent us to attribute several meanings to the principle of transparency, hence my assumption of wrongfulness for this such-fits-all interpretation of transparency being possibly controversial. However, if we accept that transparency can be justified by such diverse grounds, we

It would therefore seem necessary to better identify some nuances of transparency that might fall within the remit of the concurring principle of openness when interpreting the GFLR[164]. It has to be preliminarily remarked that the distinction between the principles of transparency and openness is unclear. Understanding this relationship is not a mere exercise of legal interpretation, but it is crucial to correctly identify the scopes and the limits of transparency/openness measures in the newly amended food law. On the basis of their interpretation, authorities will take decisions regarding the extent to which data will be disclosed, possibly challenged before the CJEU which, in turn, will confront with the same interpretative matter if it decides to maintain its principle-based approach.

EFSA programming document 2020-2022 (EFSA, 2020) seems confused as regards the use of this terminology. First, it gives prominence to the principle of openness (p. 11). In other passages of the same document the two terms are used as substitutes ("transparency/openness", p. 13). Then, the paper justifies the publication of the non-confidential version of applications dossier as an "openness" measure (p. 111). Finally, it refers to "openness and transparency" as they where different (p. 130).

To finally clarify their remit, let us now discuss four approaches to transparency and openness - displayed in the picture below - that can be found in the literature about food safety documents and data.

might end up in having no clue about the "true" meaning of transparency (hence, the generation of legal uncertainty) and potentially contradictory interpretations when measures justified by the same principle do not synergize or clash with conflicting interests

[164] I have already attempted to discuss this topic in a concise work (Sapienza, 2019), but my conclusions were limited due to the ongoing legislative process at that time

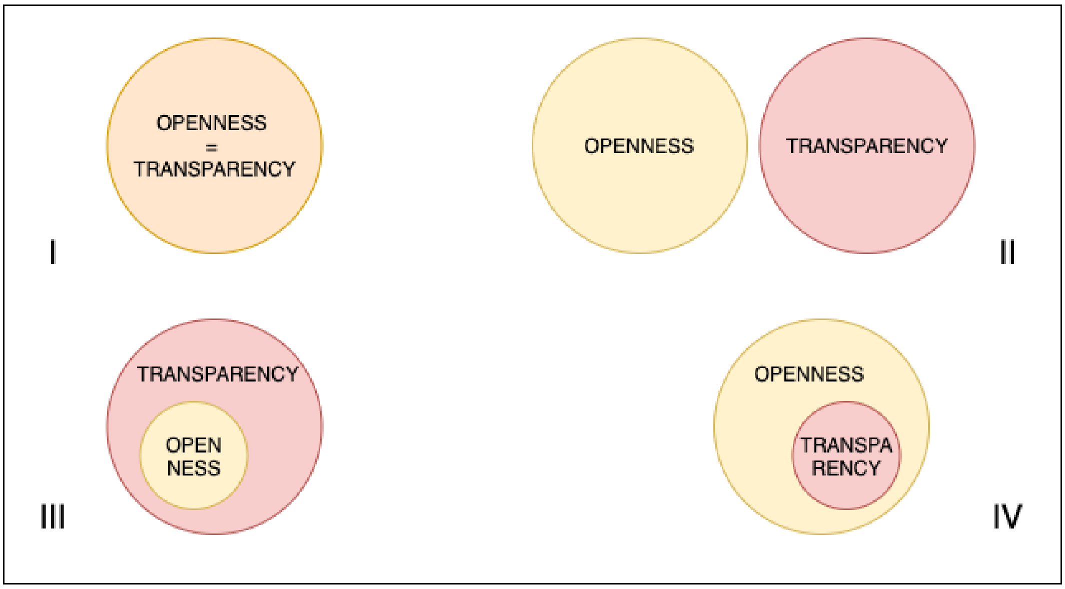


Figure 3.3: Four approaches to Openness and Transparency of Food Safety data

I. First, openness and transparency are commonly used as perfect substitutes when describing "good governance" measures indented to promote the deconstruction of layers of opaqueness and secrecy in EU decision-making (Lodge, 2003). It might be thus claimed that there is no major difference between the two concepts since they are both aimed at supporting democracy (Alemanno, 2014). The CJEU has interpreted these two concepts as synonyms when discussing Article 15 of the Treaty of Functioning of the European Union[165]. As already noted, in *Turco*, the CJEU stated that "openness [...] contributes to strengthening democracy by allowing citizens to scrutinize all the information which has formed the basis of a legislative act" [paras 41-31, 59-61]. In *Bavarian Lager*[166], the CJEU pointed out that Regulation 1049/2001 "is designed to ensure the greatest possible transparency of the decision-making process of the public authorities and the information on which they base their decisions" [para 49], thus implying little or no difference between the two terms. While this interpretation is largely confirmed in decision-making processes, it worth noticing that it does not fit reactive or proactive data disclosure measures for risk assessment purposes, whose outcomes are "scientific opinions" rather than "decisions" or "acts". When data are made available to the public to allow the cross-validation of EFSA find-

[165] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1. Article 15(1) states that "[i]n order to promote good governance and ensure the participation of civil society, the Union institutions, bodies, offices and agencies shall conduct their work as openly as possible"

[166] Case T-194/04 Bavarian Lager v Commission [2007] ECR II-3201

ings (for instance, as requested by IARC), the scientific nature of third parties' contributions is included within the remit of the "democratic scrutiny" of EFSA's work, as if the information at stake was entirely and uncontestedly owned by EFSA.

II. A second approach, at the other extreme, argues that, at least in food safety governance, transparency and openness differ significantly. On the one hand, openness concerns all the activities of the EU institutions (thus, including EFSA) and access to documents that are produced by EU agencies in the exercise of their duties. On the other hand, transparency justifies the release of information (and data) that concerns the activities carried out by private parties (Conte-Salinas and Wallau, 2016, p.582). In their view, the difference between the two principles is given by the data owner (public bodies vs private entities) and the nature of the documents to be released. However, we noted that, considering the increased weight given to access and distribution measures in the CJEU case law and in the Transparency Regulation, such monolithic approach to ownership is not always convenient, at least in light of the definition of data ownership that was given in the Introduction.

III. A third perspective may argue that transparency is the leading principle of food safety data disclosure measures and, therefore, it encompasses openness. This is due to multiple mentions of transparency (including the whole section II of the GFLR) in the provisions which mandate publications of data. Openness, instead, is used as synonymous for "inclusiveness" and plays a marginal role only in scientific consultation of third parties ((Alemanno and Gabbi, 2016, pp. 179-189), art. 32c and 32d of the amended GFLR) with no direct effects over information disclosure. Instead, it is worth reminding that EFSA's opinions do not consist of binding legislative acts, but should be conceived as politically-neutral evidence-based research. The kind of inclusivity that one can imagine to be promoting democracy is not the same as the one of people's indirect participation to decision-making processes. Some scholars have argued (Alemanno and Gabbi, 2016, p. 216) that technical advancements and the culture of "open data" has democratised science by giving citizens and stakeholders the possibility to intervene and make their voices heard. While recognising that these individuals may speak "louder" than in the past thanks to *openness-as-inclusivity* initiatives including open data, only qualified third parties can have sufficient expertise to actively participate the review of scientific evidence[167]. Therefore, "open data" attempts

[167] Moreover, other scholars (Lynch, 2016, p.146) have argued against direct effects of democratic mutations in the "knowledge economy" on the quality of democracy in a given society. Democracy may be enhanced if citizens become active part of data-driven decisions, strategies and benefits that knowledge economy originates (Durante, 2019, p.187). Although our scenario is not directly linked to the knowledge economy given by Lynch, his approach to data and democracy seems appropriate

might fail in their alleged final goal, i.e. closing the gap between (perceived) technocratic EU institutions and citizens.

IV. A fourth possibility can be then considered. Openness might be a general principle discouraging secrecy and enabling EU institutions to have greater legitimacy and to be more effective and accountable to EU citizens. As we observed in *Tweedale* and *Hautala*, the CJEU has stated that the disclosure of scientific data contributes to an *open* (emphasis added) discussion, especially towards areas of scientific uncertainty and divergence, and fosters trust in EU institution [*Tweedale* para 75, *Hautala* para 60]. In this view, openness encompasses transparency, which, in turn, inspires sector-specific reactive or proactive measures - such us access to documents and data disclosures - that facilitate citizens' access to information held by EU institutions (Alemanno, 2014) in light of the general goals enshrined by openness. A major drawback of this interpretation is *mutatis mutandis* the same that affects transparency when encompassing goals that are undistinguishable.

On the one hand, certain provisions mainly aim to foster a democratic oversight of the activities of EFSA by EU citizens, and in particular its relationship with commercial applicants; on the other hand, different measures allow scrutiny over information for the cross-validation of scientific risk assessment results. Difficulties in this explanations also arise when these goals overlap (e.g. in the factual background of *Hautala* case). Can we then provide for an unified rationale for these goals while acknowledging their peculiarities?

Considering the low level of trust proven by the 2018 Fitness Check, the policy goals of the Transparency Regulation and findings from the jurisprudence and the academic literature on transparency and openness, we could argue in favour of a model - represented by the picture below - in which openness and transparency measures are diverse but partly overlapping. In this model, actions that foster a democratic oversight over risk assessment procedures are closer to a "transparency" rationale, whereas those promoting collaborative forms of risk assessment fall within the grounds of "openness". Both principles operate towards a common goal, which is represented by the promotion of trustworthiness of risk assessors. As regards openness, what is at stake is the reputation of EFSA as a scientifically sound institution that provides reliable opinions; with regards to transparency measures, they should foster trust by making public data held by EFSA to ensure independence and accountability of the Authority.

to the context under discussion: even though "open data" initiatives in agri-food safety risk assessment are qualified as democratic instruments, the mere inclusion - rather than active participation - of citizens in the data pipeline does not necessarily imply an increase in democracy. Different would have been the case of other "open data" initiatives which might allow for a direct oversight of institutions (e.g. parliamentary open data)

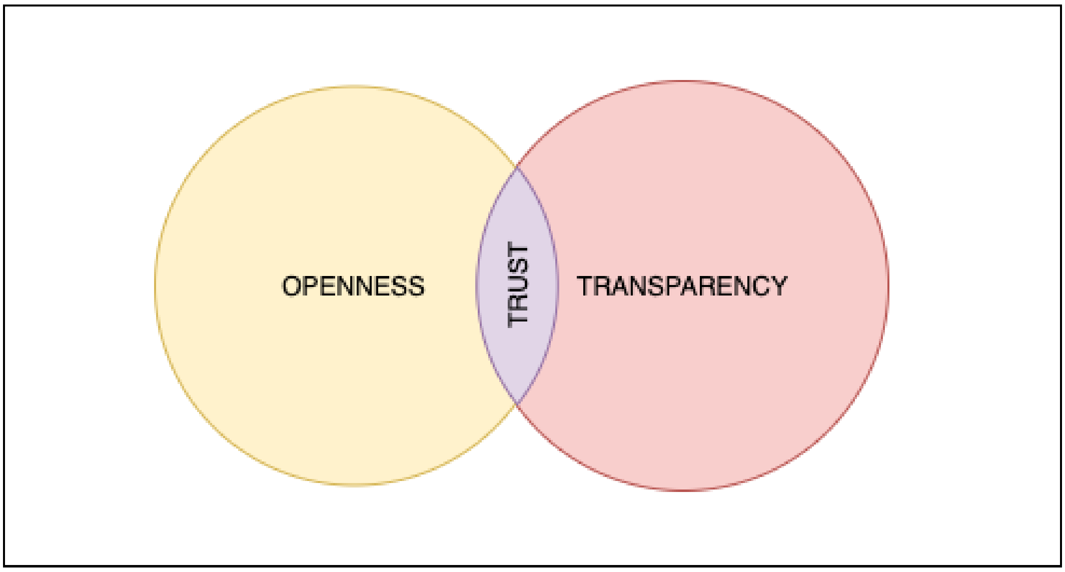


Figure 3.4: A trust-oriented approach to Openness and Transparency of Food Safety Data

The general weaknesses of other models - beside the generation of confusing lexical choices - reflect difficulties in understanding the ultimate reason why heterogeneous stakeholders should have access rights to information that are held by other parties. Our solution proposes trust as a unifying rationale.

However, the centrality of trust is not sufficient to ensure that access or distributions rights can still be justified under this perspective. In other words, while transparency-only or openness-only data disclosures are indeed justified by their respective goals found in the previous literature and in the CJEU jurisprudence, our unified trust-based solution shall also provide a unified ownership model that allows access and distribution rights under this principle. Providing such ownership model for the trust-centric proposed solution is the core goal of the next subsection.

3.4.2 A trust-oriented conceptualisation of food data ownership

One of the most notable aspects of our analysis is the issue of data ownership. Having defined this concept in §1.2.3, let us now observe how it operates at a practical level.

When analysing future trends in 2012, EFSA external reviewers[168] found that clarifying data ownership is a critical aspect, in particular when data is provided by Member States (p. 62). Reviewers noted lack of clarity on the ownership of data and once they are stored and made accessible in EFSA databases (p. 68). In particular, they concluded that contractual agreements with stakeholders might limit EFSA's ability to share data. The situation was not different in 2018, when reviewers noted "in the face of data ownership by Member States, confidentiality claims of applicants and overall conflicting provisions in existing legislation both at national and European Union level"[169]. As we are now aware of *what* is data ownership §1.2.3 and *why* it is critical, this section presents a wide range of topics and perspectives, all sharing a tentative answer to the question "*who* owns the data"?[170].

Several authors have engaged the debate surrounding data ownership in this domain. Before providing new answers, it might be useful to understand how this debate has unfolded in the last years.

On the one hand, some authors have consistently argued that data ownership remains with the "data originator". As we already noted in §2.4.2, *ex novo* generations of data by EFSA are limited, thus data originators usually being third parties. This entails that, according to Kocharov (Kocharov, 2009), data originators maintain ownership, whereas use, storage and release are regulated by EU law and contractual arrangements. In her view, the only way for EFSA to acquire ownership rights is under procurement contracts (e.g. confirmatory studies) for which EFSA retains data ownership. In the case of application dossiers, which are a major source of data for EFSA, companies maintain ownership due to the commercially sensitive nature of data - protected by confidentiality and data protection measures - and intellectual property rights.

We already noted that two kinds of measures - confidentiality and data protection - are in place to protect commercial interests of applicants or third parties. Raw data constitute a valuable asset for the companies engaged in R&D, hence the necessity of protecting this information against "free riders" or unlawful accesses. The two sets of provisions are inspired by different rationales: confidentiality aims to prevent the disclosure of secret information, whereas data protection guarantees a period in

[168] Ernst & Young External Evaluation of EFSA, Final Report 2012 https://www.efsa.europa.eu/sites/default/files/efsa_rep/blobserver_assets/efsafinalreport.pdf

[169] Ramboll and Coffey Third external evaluation of EFSA 2011-2016 Final Report http://www.efsa.europa.eu/sites/default/files/3rd-Evaluation-of-EFSA-Appendices100818.pdf, p. 12

[170] Two clarifications are necessary. First, the answers provided by these attempts are related to the technical and legal domain of food safety risk assessment; second, while this question is not explicitly included among our research questions, its preliminary assessment is necessary to formulate an answer to our second research sub-question

which other applicants cannot rely on previously submitted data unless agreed with the original data owner (Holle, 2014; Simpson, 2016).

When talking about the second sets of measures, Holle (Holle, 2014) links their existence to the exclusive right of reference to data - that we observed, for instance, as regards novel food applications in §3.2.3 - to some kind of ownership that guarantees the 5-year data protection[171]. A critical point of this interpretation consists of the other mandatory requirement for data protection, i.e. the designation of data "as proprietary" by the applicant. To maintain Holle's interpretation correct in light of this additional requirement, it can be argued that the designation of certain information as proprietary is a subjective condition that applicants claim *per se*, whereas the exclusive right to reference is an objective status recognised by the law. However, Simpson (Simpson, 2016) argues that the final version of the Novel Foods Regulation does not clarify the meaning of "exclusive right of reference" and several alternatives are discussed[172]. While a shared interpretation of this criterion is still missing, Simpson's reading is consistent with the others when attributing ownership rights to applicants due to some kind of legal *status* attributed by the law.

Crucially, "the law" is a purposeful simplification of a very complex legal framework that entails several pieces of legislations. In summary, applicants' ownership on raw data might originate from:

a) The GFLR, as regards confidentiality claims over information-types set by Article 39 discussed above;

b) Food sectoral legislation, as regards information-types other than the ones disciplined by the GFLR and mentioned in the previous sections;

c) The Database Directive[173] which grants a *sui generis* protection for the maker of the database to prevent extraction and/or re-utilisation of data if a quantitatively/qualitatively investment has been made in obtaining, verifying or present the contents of the database (Art. 7)[174]. As argued by Aplin (Aplin

[171] Please note that the article was written before the entry into force of the Novel Foods Regulation discussed above, However, for the purposes of this discussion, the requirement of exclusive right of reference to data is needed to obtain data protection also under the version of the Regulation currently in force

[172] *Inter alia*, an alternative wording present in the Novel Foods Regulation proposal had suggested an "exclusive right of reference" criterion altogether with a requirement that applicants would have been able to "demonstrate ownership of the proprietary scientific or scientific data, by means of verifiable proof." (Simpson, 2016, see footnote 19)

[173] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases [1996] OJ L 77/20

[174] Additionally, the Database Directive offers copyright protection for the selection and arrangement of the contents if they meet the requirement of being author's own intellectual creation (Art.

and Davis, 2013, para 4.4.3), ownership of the *sui generis* right lies with the maker of the database[175];

d) Trade Secrets, as defined by Article 2 of the Directive on Trade Secrets[176], i.e. information that is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; has commercial value because it is secret; has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret. As noted by an author (Simpson, 2016), proprietary data are treated in same way as trade secrets. EFSA practical arrangements for the implementation of the Transparency Regulation seen in §3.1.3 prescribe the secrecy of the information for which confidentiality can be requested as a necessary precondition for the claim.

e) Contractual agreements. Data owners could restrict access to data do not follow under the scope of other means of protections granted by the Database Directive or trade secrets by means of contractual obligations. This additional possibility has been granted by the intervention of the CJEU in *Ryanair Ltd v PR Aviation BV*[177]. Kocharov (Kocharov, 2009) affirmed that contractual arrangements between the supplier of data and EFSA are secondary forms of regulation, for which EFSA is exposed to contractual liability[178]. The same can occur for physical or legal persons to whom data are disclosed, insofar they breach the licence terms. For instance, EFSA's first disclosure in *Hautala*[179], a copyright notice was present in the cover letter introducing the release of data[180].

The outcome of this system is a rather complex legal framework - not even con-

3)

[175] My view of Aplin's assertion is that ownership of the *sui generis* right corresponds to ownership of the contents of the database, which is the object of legal protection in the *sui generis* regime

[176] Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure [2016] OJ L 157/1

[177] Case C-30/14 *Ryanair Ltd v PR Aviation BV* [2015] ECLI:EU:C:2015:10. For further comments see (Aplin and Davis, 2013, para 4.4.7), (Borghi and Karapapa, 2015)

[178] There is no limitation, however, to the raw data that need residual forms of protection as in the *Ryanair* case. Hence, all data qualify as potential object of protection by contract

[179] The correspondence between EFSA, Hautala and the other MEPs is available at https://www.asktheeu.org/en/request/is_glyphosate_safe_we_have_the_r

[180] "All persons reproducing, redistributing, exploiting or making commercial use of this information are expected to adhere to the terms and conditions asserted by the copyright holder". The referred letter from EFSA can be found at https://bit.ly/3fHlf5X

sidering the implementations of the aforementioned Directives in Member States which apply to national food safety authorities - that relies on several legal instruments for granting legal protection over valuable data. Some of these measures, like the exclusivity period for proprietary data and the *sui generis* protection for the contents of the database, present overlapping rationales, namely the goal of protecting the investment made in the gathering the protected data. Instead, the duration of such measures might range from 5 years for data protection measures, to 15 years (renewable) for the *sui generis* protection, to the undefined time span of contractual arrangements. This might cause uncertainty towards the time span needed to proceed with data releases.

On the other hand, a minoritarian group of authors have identified weaknesses in this reasoning and claimed a different approach to the question of data ownership, by identifying the emergence of a new paradigm (Korkea-Aho and Leino, 2017). When discussing the concept of ownership, authors seem to argue that a simple distinction would be that companies are granted ownership by immaterial copyright rules, whereas authorities hold physical control, i.e. possession. While the EU agencies hold submitted information, the "copyright of data"[181] belongs to companies, which can decide the conditions for data disclosure as seen in the case of replies to MEPs requesting access. The outcome is, in their view (Korkea-Aho and Leino, 2017, p. 1086), a "strained situation of shared ownership". This approach can be supported by other scholars who have referred to the "collective intelligence" made possible by the fruitful interaction with users of systems used in food safety to foster accuracy and quality of the outcome (Alemanno and Gabbi, 2016, p.213). Shared ownership might be understood as a necessary precondition of such collective intelligence.

Three major drawbacks - beside the *reductio ad unum* when discussing copyright issues only - affect this theory. On the one hand, such shared ownership shifts from a *monistic* (business operators) to a *dualistic* (EFSA *and* business operators) model. However, citizens then only play a marginal role in the view despite being the ultimate target of transparency mechanisms regardless of their rationale. On the other hand, while this approach is only focused on reactive transparency measures, a unified approach to proactive and reactive measures would be preferred also in light of the Transparency Regulation. Finally, the concept of possession is inherently inadequate to informational components, as we discussed when talking about ownership-related properties of data in §1.2.3. Despite these critical remarks, authors correctly challenge the idea of a monolithic approach to data ownership granted to companies by keeping into account the active role of EU agencies in determining *what* and *when* data can be disclosed.

[181] As we showed above, narrowing the scope of legal protection to copyright would be, in principle, reductive

While accepting the premise that a "new paradigm of ownership" is emerging and in continuity with this trend, the approach proposed by our study takes it further by looking at the Transparency Regulation and the recent case law of the CJEU more holistically.

First, it has been observed that the publication of the non-confidential version of the application dossier is now the default transparency mechanism. In ownership-based terms, this implies the shift of these units of information from private data (high rivalrousness, easy excludability) to some other form of ownership characterised by lower rivalrouness and harder exludability[182]. With this regard, the ambiguity of Article 38.1a has also to be remarked. Scientific data cannot be "used, reproduced, or otherwise exploited in breach of any intellectual property right". This appears to be in contrast with the new approach taken by Article 3 of the 2019 EU Copyright Directive[183] when paving the ground for exceptions for text and data mining[184] made by legitimate users.

Several questions arise from this joint reading. For instance, how should we determine the concept of "lawful access" when the amended GFLR does not confer any licence to use or reproduce IPR-protected data? The *lex specialis* criterion does not seem particularly helpful to determine the legitimacy of independent scientists willing to use data mining techniques over scientific information. Will food business operators be able to contractually limit the exploitation of data for legitimate text and data mining? A positive reply would seriously hamper the potential of automated literature reviews of their studies, whose growing importance has been largely discussed in Chapter 2. Finally, who will technically restrict the possibility of lawful access for the "security and the integrity of the networks and databases" where data are hosted (Art. 3(3) of the Copyright Directive)? This last point is particularly critical: while only rightholders are entitled to apply such measures, EFSA manages the infrastructure used to store the data and has the bear the burden of deciding the level of security measures, keeping into account rightholders' position while not acting on their behalf.

While the disclosure of data to the public has been welcomed as an "open data"

[182] It might be relevant to restate here that the publication of data by EFSA does not amount to an explicit or implicit permission or licence for the relevant data and information and their contents to be used, reproduced, or otherwise exploited in breach of any intellectual property right or data exclusivity rules, and the Union shall not be responsible for its use by third parties (new Article 38.1a)

[183] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC [2019] OJ L 130/92

[184] Art. 2(2) of the Copyright Directive 'text and data mining' means any automated analytical technique aimed at analysing text and data in digital form in order to generate information which includes but is not limited to patterns, trends and correlations for users having lawful access

approach in the public sphere, the doubts arising from the joint reading of these provision suggest the shift towards some kind of novel ownership model that is currently not possible to identify. However, the increased remit of exceptions in food law legislation and in intellectual property seems to prevent the attribution of a "full" data ownership on the companies submitting data, contrary to what stated by the aforementioned scholars.

Second, we noted that, in the case of the procedure for the handling of confidentiality claims, several rounds of discussions between the Authority and the applicant may occur depending on the lack of agreement between the two parties (fig. 3.1). However, EFSA is now in entitled for taking decisions regarding the proactive disclosure of data and its conclusions are subject to the jurisdiction of the CJEU. This entails - following our definition of ownership - that EFSA enjoys a limited amount of data ownership, i.e. a form of *quasi*-ownership. Such *quasi*-ownership has to be granted to EFSA due to its active role in data-related decisions as the "gatekeeper" of transparency, at least over the non-confidential and public version of the dossier for which EFSA takes decisions on the disclosure, including the "if" and the "what" has to be published. Moreover, it may be argued that, by providing so, the Legislator has purposely granted EFSA some kind of ownership rights to legitimately dispose of the data at the expense of the original data owner. The legal status of the commercial entity is somehow penalised by the expansions of EFSA's capabilities of disclosing data (emerging from the legislation) and the broad interpretation of the exceptions to confidentiality (emerging from the case-law). Therefore, even in this case a "full" ownership is not enjoyable by the commercial applicant, nor can it be granted to EFSA.

Third, the reactive disclosure of environmental information is grounded on the "foreseeability of environmental effects" criterion, justified either by the protection of human health or the need to increase trust in decision-makers. In the context at stake, the ability to foresee granted to citizens necessarily implies - at minimum - the access to data originated thanks to applicant's investment and protected as such. If our findings are correct, the ongoing datafication process will entail the necessity of reviewing also algorithms and their operational results and access should be granted on the basis of the "foreseeability" criterion. Current and foreseeable access rights are detrimental to the enjoyment of a "full" ownership by commercial applicants: if an unlimited, unjustified and indiscriminate access to confidential data could - even in theory - be given to everyone, it means that even citizens enjoy some degree of ownership in potency or "dynamically" (δύναμις, in the Aristotelic sense).

Fourth and finally, the ownership of the human informational component has been largely overlooked by previous scholars. Confidential data also include findings generated through analyses that rely on recorded food consumption behaviours. In building an ownership model, such human presence should ultimately be kept into account. Scholars in the field of privacy have described the possibility of an ownership-based interpretation of informational privacy (Floridi, 2005; Tamò-Larrieux, 2018) or personal data (Malgieri, 2016) across various domains. In summary, individuals may claim ownership over information regarding them, thus having recognised some form of *ius alios escludendi*[185]. In our context, however, this approach is unsatisfactory. While data subjects (i.e. surveyed individuals) might own their raw data, commercial applicants could claim ownership rights on the same information for the reasons seen above and both claims would be, in principle, valid. In practice, the endorsement of ownership-based theories in this context is likely to raise tensions between these parties. Moreover, if the possibility of granting access to individual data is guaranteed by means of reactive transparency measures, it looks plausible that further tensions between the public interest to process data and individual right to privacy might originate, ending in legal uncertainty as with the case of non-personal information and confidentiality[186]. Despite the lack of a full acknowledgement of ownership on personal data, the combined analysis of personal and non-personal data generates privacy-related issues that will be discussed in the next Chapter.

As none of the categories mentioned - companies, authorities, citizens and surveyed individuals - enjoys "full" ownership, a possible approach can be the one of understanding the technical and legal context of food safety risk assessment data as a distributed form of ownership in which all the entities are granted rights of accessing, sharing, using or disseminating their data. These rights, however, are not unlimited and a constant balancing exercise - as in the case of EFSA's decisions on confidentiality claims - is needed.

EFSA plays the crucial role of mediating tensions between the other parties. The Authority does not attribute larger or smaller portions of ownership to each entity. Instead, it allocates distribution and access rights according to certain criteria identified by the GFLR as amended by the Transparency Regulation while following a principle-based approach as introduced by the CJEU. As the previous analysis suggests, transparency and openness are two core principles of the EU food safety legislation. If EFSA, as argued, is entitled to allocate ownership rights in a distributed framework, these principles shall inspire their decisions also under the new

[185] A possible limitation of this approach is that all the parties involved in data protection activities also cover subjective positions typical of data protection law (e.g. data controller, data processor, data subject, third party, and so on). This reasoning, however, goes beyond subjective legal positions and should be read as a broader reflection on data ownership rather than in terms of a case-by-case analysis of data processing under a legal perspective

[186] Article 4(1)(b) of Regulation 1049/2001 prevents public access to data and documents where disclosure would undermine the protection of privacy and the integrity of the individual. In the GFLR, we have seen a "do not disclose" clause for the names of the individuals involved in toxicological studies, whereas nothing is said as regards food consumption data. In particular, specific criteria to a) identify threats to informational privacy and integrity, and b) balancing the public interest in accessing data and the individual right to data protection are missing

GFLR, also for reasons of continuity with the principle-based approach proposed by the CJEU.

Then, a clarification on the relationship between such unified model of distributed ownership and the trust-based theory of openness and transparency is needed to identify a common rationale that holds together different sets of measures allocating access and distribution rights. As remarked by the 2018 Fitness Check (*inter alia*, p. 10, 41, 45), trust is an essential component of the EU food system and, with this regard, it cannot be deemed to be external to the relationship among EFSA, the industry, and citizens, in particular when they share information. Under our data-centric and ownership-based approach, the development of trustworthy relationship between these actors is a foundational justification for distributing ownership rights when the measure granting access or distribution set broad goals, as in the case of the GFLR or access to environmental information. Similar conclusions were reached in the context of an empirical, case-study analysis on different scenarios of data sharing and distribution practices - DECODE Project (DECODE project, 2020) - in which the absence of trust was deemed to increase the likelihood of a withdrawal from an information-sharing ecosystem.

3.4.3 Foreseeable legal challenges: group discrimination, algorithmic transparency, accountability and redress

So far, this Chapter has analysed the legal framework that governs the collection, access and distribution of data used for food safety risk assessment purposes. In particular, it can be noted that the Legislator and Courts have mainly focused on solving the "transparency vs confidentiality" issue previously identified. Other challenges are foreseeable in light of the ongoing datafication process that we clarified in Chapter 2. However, little or no answer is provided by the existing legal sources for the issues described in the previous parts of that Chapter. This section aims to identify some of these unsolved concerns, whereas the next Chapter attempts to explore possible solutions.

Data Protection and Informational Privacy

Chapter 2 have underlined the presence of a human component in the data used in the course of risk assessment and explored the related risk of group discrimination. Such informational component consists of food consumption data and background information collected to perform exposure assessment. Legal and technical evidence suggests that both these "raw" information-types should qualify as personal data for the purposes of data protection law, as we have defined them in the Introduction, because the information is referred to an identified individual (i.e. the surveyed person) at the moment of collection by national authorities. Then, EFSA provides for the pseudonymisation of the individual data (EFSA, Dujardin, et al., 2019, p.13, p.19), which are made available to the public at aggregated level.

Taken together, the applicable law governing the processing of this data can be conveniently analysed by looking at the data controller as it ultimately depends on the entity that determines the purposes and means of the processing of personal data[187].

We already noted that EFSA is subject to Regulation 2018/1725, but its internal rules[188] only cover administrative inquiries and similar activities carried out by the Authority (Art. 1(2)). Likewise, the same Article 1(2) does not include food consumption information among the processed data to which the Decision applies. Being placed outside this normative implementation, I will cautiously assume that food consumption data and background information stored in EFSA database are outside the scope of this act. Following this regime, to the extent to which EFSA qualifies as data controller for the processing of personal food consumption data and background information transmitted by Member States or other third parties, all the conditions set by Regulation 2018/1725 apply. *Inter alia*, it is worth recalling that food consumption data collection is mandated by Article 33 of the GFLR, which implicitly serves as a legitimate ground for processing *ex* Article 5 of Regulation 2018/1725.

Metadata from EFSA (EFSA, 2018b) show that individual names are replaced by an identifier that are not disclosed to the public[189] under Regulation 45/2001 (now replaced by Regulation 2018/1725). From the same metadata, other data elements are of particular interest. EFSA seems to collect the "self-defined ethnic group"

[187] In the explanation below, I assume that the general public only accesses data at a higher level of aggregation in accordance EFSA Data Warehouse Access Rules. In the case of reactive disclosure of environmental information, food consumption data might be displayed in applicants' dossier at individual level. However, this case is out of the scope of the legal analysis of this Chapter due to the limitations that have been set by Article 4(1) of Regulation 1049/2001 when personal data are at stake in the course of a request of access to documents. The ECJ has addressed this issues specifically in Case C-615/13 P (*ClientEarth and Pesticide Action Network Europe (PAN Europe) v European Food Safety Authority* [2015] ECLI:EU:C:2015:489, para 57 when clarifying that, despite the mandatory strict interpretation of the exceptions to the principle of transparency, the protection of personal data prevails and prevents third parties from accessing data at individual level

[188] Decision of the European Food Safety Authority of 19 June 2019 on internal rules concerning restrictions of certain rights of data subjects in relation to processing of personal data in the framework of the functioning of EFSA (2019) OJ L 272/154

[189] In the description of these metadata, EFSA reports that "data protection" yes/no indicator contains whether the structural metadata element will be published or not (yes = will not be published, no = will be published). The full table is available in the Appendix. ORSUBCODE is the Unique subject identifier and seems to be covered by data protection

of the individual, her or his "special conditions" and whether the subject follows a "particular eating pattern". These information-types might fall within the remit of Article 10 of Regulation 2018/1725 and be processed as special categories of data if they express the ethnic origin, health conditions or dietary patterns reflecting religious or philosophical believes and are recorded as such[190].

It is necessary to clarify the positions of Member States national authorities, the industry and other researchers as regards the applicable law. Remarkable features consist of:

1. The legal position assumed by the entities at stake. When Member States are data originators, they qualify as data controllers making EFSA a data recipient for the first data processing, still regulated by the GDPR. Then, EFSA becomes data controller under Regulation 2018/1725 when it processes data for self-determined purposes. Commercial entities and academic researchers then become data recipients from EFSA - to the extent that data are still considered personal - under Regulation 2018/1725, but they apply the GDPR when determining the purposes of their own data protection activities;

2. The legitimate ground of processing. Institutions act in the exercise of authority they are vested in Article 6(1)(e)[191], whereas the industry and researchers - following access to individual-level data by EFSA - may rely on their legitimate interests (Art. 6(1)(f)) for their internal data processing activities. Different would have been the case food consumption data explicitly qualified as special categories of data, since this would have triggered the applicability of other legal basis, including statistical or research purposes (Art. 9(2)(j) of GDPR);

3. Data transmissions from EFSA. The transmission of data to third parties by EFSA, including food business operators, can occur only if the conditions set by Art. 9(1) of Regulation 2018/1725 apply: the recipient a) establishes that the data are necessary for the performance of a task carried out in the public

[190] For instance, a surveyed individual might self-declare to adhere to Islamic dietary laws. This would entail, among others, prohibitions regarding alcohol or pork. Differently, her or his recording can show adherence to Islamism without the subject self-assessing her or his religion. The way in which this information is recorded is eventually crucial. In the first case, the record of an explicit self-assessment necessarily entails the categorisation of the collected data as special category; in the second case, such speciality is only implicit since religious believes can only be inferred after a in-depth scrutiny and eventually additional data. The same can be applied to veganism and vegetarianism and food-related health conditions (e.g. coeliac disease)

[191] I am assuming that data processing may also not occur without consent. Studies carried out by national authorities are voluntary. However, individual's consent to the study shall not be confused with the one given for the data processing activities: once the first is provided to make the survey legitimate, the second is not needed if the institution is acting on the basis of its authority

interest, or b) establishes that it is necessary to have the data transmitted for a specific purpose in the public interest and the controller (i.e. EFSA), where there is any reason to assume that the data subject's legitimate interests might be prejudiced, establishes that it is proportionate to transmit the personal data for that specific purpose after having demonstrably weighed the various competing interests. At the same time, the controller shall demonstrate that the transmission of data is necessary and proportionate to its purposes;

4. The processing of sensitive data by data recipients. In the absence of consent, the industry could rely on the ground provided by Art. 9(j) (in particular, scientific research or statistical purposes) to process special categories of data for their own R&D activities. The same could be applied for academic or independent researchers. Crucially, Recital 162 of the GDPR and Article 89 allow for Member States derogations, thus making legal compliance cumbersome for international companies. Transmission by EFSA occurs under Article 9 of Regulation 2018/1725;

5. Spontaneous data transmissions to EFSA. Other parties, in particular academic institutions, might be willing to transmit independently collected data to EFSA. When this is the case, GDPR applies until EFSA proceeds with its (i.e. self-determined) activities.

Overall, the interplay between these legal instruments might seem cumbersome because the applicable law and the grounds of personal data processing change for every transmission. However, the GDPR and Regulation 2018/1725 are largely compatible when it comes to definitions and essential principles. A more concrete challenge might be the one of guaranteeing interoperability and standardisation of data when different legal regimes apply.

The use of aggregated data[192] makes all the aforementioned provisions not applicable (Recital 16 of Regulation 2018/1725, Recital 26 GDPR), as they only apply to data that are considered referred "personal" - i.e. referred to an identified or identifiable person - or considerably lower the risk for individual data subjects if they are not used to take decisions that regarding her or him (Recital 162 GDPR). Scientific opinions taken by EFSA or measures adopted by the industry do not directly refer to an individual, thus not raising specific concerns regarding particular persons.

[192] Although this thesis does not explicitly refer to anonymous or anonymised data, some clarifications are necessary. Considering the data processing practices described in Chapter 2, the amount of variables collected by EFSA suggests that the possibility of re-identifying surveyed individuals seems - at least - plausible. EFSA metadata show the collection of 40 individual variables, 31 of which are not covered by non-publication measures. For instance, studies (De Montjoye et al., 2013) showed that a small number of variables can allow re-identification, hence the need of further research on this topic and specific attention by EFSA

Perhaps, this is the reason underlying the lack of any guidance on the collection of personal data published by EFSA or within the GFLR.

While this silence and the absence of case law related to food consumption data protection might suggest that the question is not of interest or can be solved by complying with the measures reported above, the ongoing datafication process suggests that some risks linked to the security and the privacy of these data need further attention. We will therefore refrain from further analysing the compatibility of the aforementioned norms and we will focus on the identification of other issues not directly linked to this complex legal framework. In particular, when food consumption data and background information will be collected with a greater level of detail thanks to the consolidation of ongoing trends identified in Chapter 2, future challenges will involve the balancing of distributed access to these data with the protection of individual rights and freedoms. Finally, discussing the safeguards of groups against possible discriminations following the development of probabilistic models using aggregated data is justified by the multiple references to group-level analysis done on food patterns or dietary habits that might be linked to religious or ethical believes or health conditions.

Algorithmic transparency

Algorithms are placed outside the legal discourse regarding food safety risk assessment. The scope of transparency and openness as regards the use of softwares that allow advanced analytics techniques is unknown, as neither related provisions in the amended legal framework nor case law from European Courts can be safely applied. Nevertheless, it has been remarked (§3.2.1) that EFSA occasionally can obtain a copy of the programming code used for statistical analysis (in GM Food and Feed) and the relationship between computer programmes and environmental information following Courts' interpretation of transparency has been questioned (§3.4.2).

Foreseeable legal challenges in this domain necessarily revolve around the growing use of machine learning algorithms in the context of risk assessment. In particular, future challenges for transparency - yet, unsolved by the Transparency Regulation - regard the degree of institutional access to algorithms and statistical models used by the industry when drafting dossiers and, at the same time, the general, reactive or proactive access to the models used by EFSA in its risk assessment, for instance in literature reviews.

While transparency is a well-known principle governing data transmission among the stakeholders, its contextualisation with regard to algorithms necessarily implies some kind of convergence between the general notion of "algorithmic transparency" and the meaning attributed in our previous discussion. Several studies - discussed in the next Chapter - have identified around as many nuances of "transparency" with regards to algorithms and, more specifically, machine learning models, which include the interpretability of internal functioning of the statistical model, post-hoc interpretations, and so forth (Mittelstadt, C. Russell, et al., 2019). Discussion on algorithmic transparency is also displayed the Commission 2020 White Paper on Artificial Intelligence (European Commission, 2020, p. 15).

With this in mind, it is possible to identify at least two types of legal challenges. On the one hand, an area of investigation should aim to address the extent to which, in light of the principles of openness and transparency, algorithms and machine learning models should be made available to the public in a way that is necessary and proportionate to the consequential limitation of intellectual property rights (De Minico, 2019)[193]. On the other hand, a natural progression of "algorithmic transparency" studies should see how to govern their use in the domain at stake, in particular when probabilistic models are used to draft dossiers submitted to EFSA in support of applications for regulated products.

Accountability and Redress

Accountability is closely related to the issue of transparency. The EU Commission has underlined that "[t]he lack of transparency (opaqueness of AI) makes it difficult to identify and prove possible breaches of laws, including legal provisions that protect fundamental rights, attribute liability and meet the conditions to claim compensation" (European Commission, 2020, p.14). Although the document was related to certain AI applications that differ from our domain, Commission's paper seems sufficiently broad to raise the legal challenge of accountability also in the context of food safety risk assessment.

The GFLR has brought attention on the "justiciability" of EFSA's decisions on confidentiality. However, no case law can be found on its scientific opinions and, in the absence of specific provisions, the justiciability of its technical conclusions are at least disputable. Scholars (Alemanno and Gabbi, 2016, p. 41) have argued against the possibility of a judicial review of EFSA's scientific opinions since they do not have a binding nature, do not aim at creating effects *ratione personae* and are not

[193] "As regards the functional transparency of the algorithm, it is satisfied by the presence of a selective disclosure, that covers only the most relevant features of the algorithm, to allow interested parties to understand the goals of the predictive mechanism. A full knowledge of the algorithms would unduly erase intellectual property rights granted to its legitimate owner, without contributing to the goal of the disclosure, as making available to the public the whole functioning of the algorithm would only benefit expert people. Therefore, this extreme position would hamper without creating any advantage: it has to be rejected due to the lack of necessity and proportionality" (*ED.* author's own translation. Original language: Italian)

applicable *erga onmes*. Only safety risk managers carry the responsibility for their (administrative) decision. This holds true also for other documents (Opinions, Reports, Conclusion, and so on) produced by the Authority.

The CJEU has confirmed the non-binding nature of EFSA scientific opinions in multiple occasions[194] and only "manifest error, abuse of powers or clear excess in the bounds of discretion" can fall within the scrutiny of the Court (Gabbi, 2008)[195]. As a result, the CJEU cannot verify the scientific reliability of EFSA's outputs either for the lack of direct effects over entities which could challenge them, or for a general principle of scientific independence and excellence of the Authority. As noted in *Pfizer* case [para 198], the Commission is responsible to assess the soundness of the opinion delivered and act accordingly.

Commentators (Alemanno and Gabbi, 2016, p.229) have noted that, hypothetically, EFSA non-contractual liability will be realised only if three conditions, i.e. *unlawful behaviour* (i.e. sufficiently serious breach of law), some *measurable damage* and the *evidence of a causal link* between the conduct and the damage - are met. Only in the *Dow* case, applicants tried to provide evidence for loss of reputation due to an incorrect scientific assessment, but the Court considered the plea inadmissible for failing to provide qualitative and quantitative details about the alleged damage.

We already discussed how the deployment of machine learning methods might generate failures which are intrinsically linked to the probabilistic nature of the statistical model. Paraphrasing what the Commission observed and findings from case law, these mistakes might be harder to subsume under the typical categories of liability (e.g. error or negligence) also in our domain. Let us imagine the scenario in which some kind of regulated product is deemed to be safe thanks to machine-learning generated predictions submitted to EFSA by a commercial applicant. The Authority considers both the software and the results reliable by accessing the source code and by making it run in different configurations. However, probabilistic results always embed a certain degree of uncertainty. Certain techniques[196] might reduce

[194] In Case T-311/06 *FMC Chamical and Arysta Lifesciences v. EFSA* [2008] ECLI:EU:T:2008:205, Court's general order noted that "only measures definitively laying down the position of the institution on the conclusion of that procedure are, in principle, measures against which proceedings for annulment may be brought. It follows that preliminary measures or measures of a purely preparatory nature are not measures against which proceedings for annulment may be brought" (para 43). The exact same wording was used in Court's order in Case T-312/06 *FMC Chemical v. EFSA* [2008] ECLI:EU:T:2008:206 para 43 and Court's order Case T-397/06 *Dow Agrosciences v. EFSA* [2008] para 40. All the three cases were decided on June 17, 2008 (Alemanno and Gabbi, 2016, p. 222)

[195] Also, EFSA liability is limited to contractual liability (Art. 47(1) GFLR) and for the damages caused by its servants (Art. 47.2)

[196] *Inter alia*, *k*-fold cross validation ensures that the statistical model is generalisable to new and unprecedented data by minimising the possibility of overfitting; selecting larger and inclusive

this margin, but, to date, there is no guidance on how to implement them.

A foreseeable legal challenge might be identification of the entities that should be responsible for providing directions and strategies for the deployment of machine learning algorithms and which principles should steer their development in a way that minimises risks, which range from the inclusion of harmful products within the lists of approved substances to the reputational damage that undertakings might face when a safe product is wrongly deemed unsafe. Also, building robust redress mechanisms that allow the scrutiny of algorithmic-supported decisions characterised by for probabilistic failures should be considered one of the foreseeable normative challenges.

3.5 Chapter Synopsis

The investigation of openness and transparency carried out in this Chapter has shown the implications of the 2019 amendment to the GFLR and sectoral legislation in the field of data collection, standardisation and divulgation, read in light of the jurisprudence of the CJEU and academic commentaries. It has to be preliminarily observed that, as these measures will entry into force in March 2021, making strong claims at the time of writing on their efficacy would be premature. Therefore, these final comments have to be read as an attempt of framing the current state of EU food safety legislation as regards the gathering and the analysis for risk assessment purposes.

First, a certain degree of convergence has to be noted among the Legislator and the Courts. While the former has mainly been keen on empowering proactive measures to ensure a wide dissemination of scientific data, the latter have intervened to clarify the scope of reactive transparency measures in a way that was consistent with the goal of granting access to environmental information to the furthest extent possible without limiting undertakings' legitimate interests.

Taken together, the direction taken by rule-makers and the judicial seems oriented towards the acknowledgement of the greater importance of data in the scientific assessment of food-related products, including regulated ones, that has been stressed in Chapter 2. Data disclosures are encouraged due to their relevance both towards

training data reduces the likelihood of biases emerging from underpopulation or overpopulation of samples; several techniques, including *k*-means and *k*-medoids, adopting the right number of clusters - usually called *k* - in clustering problems strikes a balance between the extreme accuracy of having one cluster for each data point (over-representativeness) and a single *one-fits-all* cluster inclusive of all data points (under-representativeness) the goal of promoting a democratic scrutiny over risk analysis and collaborative forms of risk assessment in which independent scientists are encouraged to provide their own findings. Remarkably, this second goal has been pursued following data-related scandals and pressing calls for better data quality.

While enhancing data dissemination measures, the wording used by the Legislator and the Courts has reflected these different goals in the principles of "openness" and "transparency". However, different and occasionally confusing uses of these words can be found in the language of EFSA and academic commentaries, thus hindering the identification of the rationales underlying specific measures. The discovery of their grounds shall not be conceived as a trivial hermeneutic exercise. In light of the principle-based approach proposed by the CJEU, a sound interpretation of the scopes of openness and transparency is needed to increase legal certainty under the new framework.

With this goal in mind, we provided a unified justification for their implementations, i.e. the principle of Trust. Its use as a foundation for legal interpretation is not entirely new. It was explicitly mentioned as one of the pivotal aims of the new food safety legislation. However, our attempt has been towards reconciling this principle with the ones already existing in the previous framework and discussed in the case law - i.e. openness and transparency - when the individual goals of the each of them are overlapping and single-perspective interpretations are not sound, as in the case of the jurisprudence discussed above.

From a *de iure condendo* perspective, we have broaden the scope of our analysis on the new legal framework to critically emphasise a "new paradigm" of data ownership that emerges from our findings. Enhanced openness and transparency principles, unified by a trust-based rationale significantly change the previous statements that attributed data ownership to the originator, i.e. the commercial entity submitting data. While multiple legal instruments usually confer intellectual property over data to the food business operators, reactive and proactive measures suggest that the ownership of these data as defined in the Introduction shall be conceived as distributed rather than centralised. In fact, under the new legal framework, EFSA is in charge of attributing access rights by proactively or reactively distributing information as mandated by the law and, following the proposed interpretation, under the principle of trust. The increasing remit of transparency and openness measures - above all, the publication *by-default* of the non-confidential version of applications dossiers and data - further decreases the monolithic interpretation of data ownership discussed by previous literature.

Finally, when analysing the new legal framework, we noted that among the three informational components identified in Chapter 2, only the second - non-personal information - has been heavily regulated. Such exclusivity is possibly due to its significant economic dimension and the noticeable conflict of private and public interests in gaining access to these data. Overall, the current legal framework appears quite limited in addressing other issues - individual and group informational privacy, algorithmic transparency, accountability and redress - linked to the ongoing datafication process. While acknowledging the presence of certain identified pillars - openness, transparency, trust - our investigation shall not ignore the limitations of the current legal framework and provide for inclusive solutions that encompass all the facets of technical advancements in food safety risk assessment.

4

The ethical perspective: AI Ethics initiatives and charters for a trustworthy innovation

4.1 Big Data and machine learning in food safety: the necessity of ethical contributions

4.1.1 The role of ethical thinking in food safety datafication

So far, this dissertation has discussed technical and legal advancements in food safety risk assessment occurring in the EU. Chapter 2 has identified an ongoing "datafication" trend of risk assessment activities, which consists of a growing use of Big Data and data analysis techniques in various contexts, together with a systematic description of three "informational components" that characterise such datafication, namely personal, non-personal and inferred data. In particular, inferences are now made possible by the abundance of data available for analysis and the promising deployment of machine learning techniques in this domain. Chapter 3 has reviewed the legal framework regulating data collection and information sharing practices among the stakeholder involved by providing insights about the amendments to EU food law brought by the 2019 Transparency Regulation and by discussing the recent case law of the CJEU. While identifying a certain disagreement on the notions of openness and transparency, Chapter 3 has proposed a trust-based interpretation of some data-related rights (e.g. access, distribution, analysis) which, taken together, compose the basis of a distributed data ownership model. It has also welcomed the innovations brought by the Transparency Regulation under such trust-based perspective, but limitations have been found in the lack of any guidance regarding the use of probabilistic models in food safety domain, which appears necessary to stem some threats due to the non-deterministic nature of the results of the analysis.

As explained in §1.4, the methodology of this thesis relies on ethical contributions to fill the normative gaps that might hinder the adoption of trustworthy solutions for the deployment of Big Data analysis and machine learning techniques in food safety risk assessment practices. While the current legislative framework seems appropriate in handling access and distribution rights over the large quantities of data that are available for analysis, the realm of cutting-edge data analytics techniques has been largely overlooked by lawmakers. Risks identified in §2.4.3 - which include the possible lack of accountability frameworks, the emergence of data-driven fallacies, the absence of redress mechanisms, and so on - might preclude individuals to trust risk assessors and the industry in a similar fashion to the aftermaths of the Monsanto Paper scandal for what concerned data inaccessibility and scientific uncertainty.

Despite the lack of future-proof normative solutions, food safety data are now heavily regulated in the EU and the amendments brought by the Transparency Regulation, to be read in conjunction with the recent case law of the CJEU, cannot be ignored. At the same time, traditional legal interpretation criteria (e.g. analogy) might be unsuccessful in finding answers among normative sources that do not keep into account the dynamics of the ongoing datafication process, in particular as regards the deployment of non-deterministic algorithms.

Therefore, this Chapter shifts from the heavily-regulated and well-studied dimension of data gathering, storage, and transmission, to the partly unknown realm of data analysis, in particular in light of probabilistic modelling and machine learning. Ensuring continuity between these two dimensions is necessary to prevent fragmentation among the conceptual bases of the Roadmap that will be proposed in Chapter 5.

To ensure coherence, ethical contributions might be useful to interpret and align the existing legislation to principles that have been discussed in the field of AI ethics purposively drafted to identify the extent to which the deployment of AI solutions is consistent with the legislation in place, disrupts the current legal framework or suggests further legal thinking. Then, it would be possible to select certain principles, on which a significant degree of consensus has been reached, to draft a list of principles that might contribute to unleash the power of Big Data and their analysis in a trustworthy way also in the domain of food safety.

Following a short introduction of their role in AI governance and justifications on their choice (**§4.1**), this Chapter aims to introduce and discuss some prominent "AI Charters"[197] (**§4.2**). Then, before introducing our Roadmap in Chapter 6, the methodology is refined to prevent possible fallacies and to clarify how the Roadmap relates to data governance while offering an ethical perspective (**§4.3**).

4.1.2 The role of ethical thinking in the current debate on AI Governance

AI governance has been defined as "one of the hottest topics in contemporary institutional debate" (Pagallo et al., 2019). The disruptiveness of AI systems raises ethical questions regarding their uses, the minimisation of harm and the promotion of "Good AI". This has led to a significant increase in the publication of AI charters, guidelines and recommendations (Hagendorff, 2020). These documents come from multiple sources, including the industry, academia, multi-stakeholder *fora* and public decision-makers.

A complete discussion of all these documents falls outside our scope[198]. Instead, we can rely on some academic reviews (Fjeld et al., 2020; Jobin et al., 2019; Morley, Floridi, et al., 2019) that have grouped and labelled these documents according to their origin or the principles mentioned therein. First, we could focus on identifying the role of such ethical contributions - regardless of their sources - in the context of AI Governance.

The current debate in AI ethics has critically discussed the proliferation of these documents. The question of what constitutes ethical AI and, in turn, what principles should steer their development has led reviewers to identify common traits in previous works. For instance, the AI4People initiative (AI4People, 2018) - further discussed below - has identified consensus towards certain principles in previous studies and chose to adopt only one new principle - Explicability - since it had not been previously identified. This methodology avoids both possible overlaps among values (including conflictual ones) (Floridi and Cowls, 2019) and the fragmentation of principles into smaller components that might prevent a clear understanding of

[197] The use of this term is purposively broad and includes any kind of document, regardless of the name - guidelines, reports, working papers, and so on - that aims to identify ethical principles to steer the adoption of AI techniques

[198] An updated list of the available Charters is available thanks to the efforts of Algorithm Watch, a German non-profit organisation discussing the societal implications of AI. Its AI Guidelines Inventory is available at `https://inventory.algorithmwatch.org`

each proposed value.

Ethical charters mostly aim to identify values that shall be used when designing and deploying socially-acceptable AIs (Mittelstadt, 2019, p.5), also in the sense of normative constraints (Morley, Floridi, et al., 2019). Therefore, principles enshrined in AI charters are both initiator- and context-dependent. On the one hand, a developer community (initiator) might choose to adhere to certain ethical standards (let us say, "Explicability" to prevent the risk of opacity) and behave accordingly (for instance, by releasing source codes, training and test sets) while a company might struggle to recognise the same principle (for instance, due to the need of preserving its business secrets). However, both entities share a "design" perspective. Instead, public institutions might agree on the principle of "Accountability" to prevent immunities from the malicious use of AI systems while adopting a "deployment" perspective (Smit et al., 2020). On the other hand, when analysed from a technical standpoint, AI charters approach AI holistically and try to find principles that can be used from the design to the deployment (or post-execution) steps[199]. Such holistic approach is necessary to prevent the oversimplification of ethical principles by translating them into "computable and implementable" concepts lacking of in-depth understanding (Mittelstadt, 2019).

Since AI technologies are pervasive towards multiple industrial sectors and disciplines, AI charters tend to adopt a broad perspective when analysing the state-of-the-art and prescribing recommendations for the implementation of their principles in practice. This can be observed from the definitions adopted by the Charters, which describe AI as "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" (European Commission, 2020, p.1) or identifying Strong and Weak AIs[200]. Occasionally, specific attention is given to controversial subject matters, including AI justice[201] or lethal autonomous weapon systems (Villani et al., 2018, p.125), especially when manufacturers of AI systems in these market sectors take action. In general, however, AI charters adopts an horizontal dimension approaching AI in all its manifestation.

[199] For instance, "Accountability" principle can be associated to design, in terms of the development of systems that allow an investigation of failures, or execution, as regards the moral or legal responsibility for the use of the system

[200] "Strong” AI means that AI systems have the same intellectual capabilities as humans, or even exceed them. “Weak” AI is focused on the solution of specific problems using methods from mathematics and computer science, whereby the systems developed are capable of self-optimisation" (BMWi, 2018, p.4)

[201] See, *ex multis*, European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment released by the European Commission for the Efficiency of Justice available at https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c

From a legal perspective, instead, the relationship between AI charters and existing normative frameworks can be expressed - following Floridi's interpretation of the role of ethics in this debate (Floridi, 2018) - either as a challenge to the existing legislation to be used in a *de iure condendo* perspective ("hard ethics") or as what ought and ought not to be done over and above the existing regulations ("soft ethics"). The choice between "hard" or "soft" ethics consideration ultimately depends on multiple factors, including the degree of regulatory interventions in certain fields and the nature of the entity that drafts and publishes the document. AI Charters often contain principle-based recommendations for their implementations[202]. Other authors have also noted that ethics lacks of democratic representativeness in rule-making and checks & balances mechanisms to preserve the rules of law [203]: from the domain of bioethics (Tallacchini, 2015), these considerations have been extended to data protection and AI governance (Van Dijk and Casiraghi, 2020)

Whether or not these suggestions are attempts to foster or suppress amendments to existing legal frameworks or novel forms of legislation depends on multiple factors, including the risks emerging in certain areas[204]. At the same time, they occasionally identify what form of governance (e.g. "hard law", "soft law", self-regulation or in-between solutions) AI should be given[205]

4.1.3 The convergence around institutional AI charters

As already discussed in the Methodology section (§1.4), our approach consists of adapting high-level documents to the technical and legal domain reconstructed in the previous Chapters. To do so, it is first necessary to identify inclusion and exclusion criteria for the ethical Charters to be analysed.

[202] *Inter alia*, see the methodological premises of the HLEG discussed below. A notable alternative approach consists of the "human rights" perspective (Mantelero, 2020, p.3). Differently from the principle-based one, the human rights framework "can provide a universal reference for AI regulation, while other realms (e.g. ethics) do not have the same global dimension, are more context-dependent and characterised by a variety of theoretical approaches". Unfortunately, as noted in the Introduction, the existence of a right to safe food in the EU is highly contested. When referring to the human right to health and well-being, the existing EU food safety legal framework also contemplates the freedom to conduct a business and, as we have seen, these rationales occasionally clash in data-related matters. Therefore, while acknowledging the fundamental relevance of the human right approach in the AI ethics debate, it might not be convenient to draw conclusions by adopting this perspective for the purposes of this dissertation

[203] Remarkably, these authors refer to a form of "hard" ethics rather than considering "soft" versions of it

[204] For instance, the EU AI Strategy discussed below states that "[F]or high-risk cases, such as in health, policing, or transport, AI systems should be transparent, traceable and guarantee human oversight"

[205] Possible implementations of this study are discussed in §5.3

Considering the territorial scope of this analysis, our methodological choice falls on documents published by EU institutions and Member States. The centrality of EFSA in collecting and analysing Big data also by means of probabilistic algorithms has been remarked in previous Chapters. As discussed, the Authority is active in data standardisation, manages data access and distribution rights, and has to be trusted when fulfilling its institutional tasks. Member States play a crucial role in collecting food consumption data for risk assessment purposes and populate EFSA databases. They are also a one-stop-shop for the industry data submissions and have access to most of the information at stake. Therefore, we will mostly rely on institutional Charters released by Member States and the European Commission.

Crucially, some of the Charters also contain recommendations about possible regulatory implementations for non-institutional undertakings or about public investments intended to foster AI development and deployment[206]. While such recommendations might be too detached from the ethical scope of this analysis and diverse among the documents, the scope of underlying principles seem to be consistent throughout the Charters. Instead, an enquiry aiming at including policy or investment recommendations may require a broader evaluation of public funding policy and political convenience to be methodologically sound.

Other documents released by interdisciplinary groups of scholars or international initiatives have been selected as auxiliary sources. These documents bridge the gap between the institutional perspective and the AI ethics discourse, thus providing for further thinking on the significance of the principles discussed in the first sets of documents. In some cases, these papers have been used as sources for the drafting of institutional Charters[207]. We will include among the auxiliary sources some notable examples with the goal of ensuring plurality and diversity of initiators and addressees.

[206] For instance, the EU Commission HLEG has released - together with their AI Charter - a document called "Policy and investment recommendations for trustworthy Artificial Intelligence" which discusses the implications of AI with regards to other societal and financial aspects https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence. Similarly, the AI Italian strategy discussed below also contains some policy indications.

[207] See, for instance the reference to AI4People initiative made by the EU Commission High-Level Expert Group on AI (p. 11) or the endorsement made by the EU Commission White Paper On AI to the work done by the the Expert Group (p.3)

4.2 Guidelines and initiatives on the deployment of Artificial Intelligence and machine learning systems

4.2.1 Institutional charters

Primary sources of our investigation consist of AI ethical Charters published by EU and Member States institutions. Among the latter, Germany, France, the Netherlands, and Italy have been selected for their institutional activities on AI governance. The United Kingdom has been excluded due to its recent withdrawal from the European Union.

European Commission Communications: "Artificial Intelligence for Europe" (European Commission, 2018) and "White Paper On Artificial Intelligence" (European Commission, 2020)

European Commission's Communication "Artificial Intelligence for Europe"[208] lays down the EU approach to an effective and trustworthy deployment of AI technologies in Europe. The document covers a wide range of topics, including the way in which AI is already changing our life, the research directions, and key areas of investments. This document comes at the end of an EU-wide dialogue that involved a cooperation agreement[209] and the setting up of a High-Level Expert Group (HLEG, discussed later) in 2018, whose conclusions were endorsed in a subsequent Communication by the Commission in 2019[210]. Moreover, these documents has to be conceived as preliminary works for the 2020 Commission White Paper on Artificial Intelligence[211] (Pavon and Gonzalez-Espejo, 2020, Ch. 2.02A).

[208] Communication From the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions "Artificial Intelligence for Europe" (OM/2018/237 final) https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe

[209] EU Commission, "EU Member States sign up to cooperate on Artificial Intelligence" https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence

[210] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Building Trust in Human-Centric Artificial Intelligence (COM/2019/168 final) https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52019DC0168

[211] EU Commission, "White Paper On Artificial Intelligence - A European approach to excellence and trust" (COM/2020/65 final) https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Taken together, these policy documents highlight a clear direction for EU AI[212] and data governance, which aims to minimise risks and promote opportunities to create a trustworthy ecosystem. In its development, the EU approach to AI seems to progressively endorse a regulatory trend, yet limited for AI systems that pose high risks (White Paper, p. 3). Threats for safety, consumer and fundamental rights might derive from the sector in which AI is deployed (e.g. healthcare, transport, energy, etc.) and the characteristics of the system itself (e.g. the possibility to produce legal effects on individuals). These two criteria identify sensitive areas that call for detailed forms of regulation (White Paper, p.17). As regards areas other than the critical ones, the Commission has progressively refined its approach without explicitly calling for "hard" regulation. For these areas, we can rely on the observation by Pagallo and colleagues (Pagallo et al., 2019), according to whom "the debate is about how to complement and strengthen the existing regulation".

From a technical perspective, machine learning is defined as a subset of AI in which "algorithms are trained to infer certain patterns based on a set of data in order to determine the actions needed to achieve a given goal" (White Paper, p. 16), hence the necessity of adapting such high-level AI framework to the peculiarities of the technicalities that we described in Chapter 2. *Mutatis mutandis* some technical considerations of the Commission shall be deemed extendible to the technical advancements observed in our domain.

From a legal perspective, the food safety domain is not an area that meets the two criteria used to identify areas that pose risks to individuals[213]. We already noted that EFSA's opinions neither have a significant impact on individuals, nor do they directly pose risks to fundamental rights. Instead, according to the way EFSA's conclusions are substantially and procedurally drawn, they tend to take into account groups of individuals that present similar eating behaviours and are inserted within decision-making processes for which EFSA *supports* decisions that might impact on fundamental rights (in particular, the right to health). More importantly, the food and chemicals industries are never discussed in terms of "AI high-risk" market sectors, thus preventing any expectation of tailored regulatory solutions for the industrial side of our domain[214].

[212] Artificial Intelligence is described as "systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals" (Artificial Intelligence for Europe, p. 1)

[213] Instead of excluding *a priori* any interest in agri-food safety due to the lack of (high) risks, identifying criteria for a trustworthy deployment of machine learning techniques is still necessary due to the absence of trust in the system already shown and discussed. What is at stake is not the necessity of regulating the deployment of machine learning, but how a principle-based discussion can foster trust in the system

[214] This is an additional justification for the "soft ethics" nature of the Roadmap presented in this thesis

At EU Commission, an agreement has been reached on seven core principles to steer future regulation of high-risk AI systems.

- Human agency and oversight. The Communication calls for control measures over the functioning of AI systems. Adaptability, accuracy and explainability of AI machines are mentioned together with human-in-the-loop, human-on-the-loop, or human-in-command models[215];

- Technical robustness and safety. Security, reliability and robustness are key to ensure the capability of the systems in the handling of errors or fallacies. Two necessary prerequisites - reproducibility of the results and safety/security-by-design approaches - are also emphasised;

- Privacy and data governance. Data protection and privacy are associated with the need of constructing databases that do not reflect biases or generate inaccuracies. As noted by commentators, this approach calls for a new understanding of data protection tools that is detached from the individual and transactional conceptualisation of the current regulatory framework and can synergise with other principles, such as human oversight, transparency, and fairness (Kuner, Cate, et al., 2018);

- Transparency. Algorithmic transparency comes with the traceability of AI systems (log, documents, data gathering and labelling procedures) and explainability/explicability of the logic underlying the decision, as well as other factors that led the deployment of the algorithms (e.g. business model);

- Diversity, non-discrimination and fairness. Datasets can be imbalanced or poor quality and produce biases and incompletenesses. Design, dialogue and participatory solutions are necessary to include all the stakeholders that might be affected by the system;

- Societal and environmental well-being. This principle relates to the societal and environmental externalities of AI systems, to be understood also in light of UN SDGs;

- Accountability. This principle should ensure auditing (*ex-ante*) and redress (*ex-post*) mechanisms to identify potential risks and to prevent lack of responsibility for the use of AI systems.

[215] For further insights on this models, see also (Quintarelli et al., 2019) and the description made by the HLEG introduced below

German Federal Government: "AI Strategy" (BMWi, 2018)

The German approach to AI is described by a joint documents signed by the Ministries of Education & Research, Economic Affairs and Energy, Labour and Social Affairs[216]. The Strategy defines AI from the well-known "strong" vs "weak" perspectives (S. Russell and Norvig, 2010, Ch.1)[217]. The document does not present an explicit list of values that corroborate the existing legislation and calls for amendments of the current regulatory framework when modifications seem needed following the necessary evaluations (p. 39). However, the document shows adherence to ethical principles in consistency with German "liberal democratic constitutional system" (p.8). Such integration should be realised by a broad societal dialogue. It is then possible to identify some steering principles throughout the Charter:

- (Data) Security. It is presented as a functional component of the societal benefit, both for the collectivity and for German attractiveness for export (p.8)
- Explainability. This principle is understood as a way to prevent opacity of "black-box" algorithms. Explainability is functional to ensure trust in AI systems and to assess their compliance with legal requirements (p. 16)
- Transparency. This principle is partly overlapping with explainability as regards its goals (promoting trust by accessing the functioning of the model, p.16), but it seems mostly referred to the results of the whole algorithmic process (p.10) rather than the features of the underlying mathematical or logical model. Specifically, it is conceived as a way to prevent and challenge undue discrimination, both at individual and group level (p.38). When considering this goal, other dimensions of transparency - predictability, non-discriminatory nature and verifiability - are recommended in the "development, coding, introduction and use of AI systems (including training and application data)."
- Accountability. Trustworthiness is also fostered by the principle of accountability, which calls for measures introducing auditing, developing impact assessment standards and the disclosure of AI algorithms (p.38).
- Privacy and Data Protection. The German AI Strategy is keen on promoting "self-determination (particularly the right to control one's data)" and citizens' privacy (p.39.). In the area of privacy and data protection, careful recommendations are made, including the development of synthetic training data to

[216] German Federal Government, "Artificial Intelligence Strategy" https://ec.europa.eu/knowledge4policy/publication/germany-artificial-intelligence-strategy_en

[217] The Strategy also explicitly mentions machine learning approaches within its scope (p.5)

avoid bulk data collections.

French Conseil national du numerique: "For a meaningful artificial intelligence: Towards a French and European strategy" (Villani et al., 2018)

The French AI strategy document - "For a meaningful artificial intelligence: Towards a French and European strategy", also known as Villani Report from its main contributor - points out a significant number of ethical principles to steer the adoption of AI systems. Machine learning is explicitly covered by the charter as it is deemed one of the key advancements of AI (p.4). Part 5 - "What are the Ethics of AI?" - illustrates a significant number of ethical principles to follow in the development and deployment stages of AI systems. Principles are needed to maximise the collective benefit of French and European societies. Ethical recommendations are intended as principles that "occupy the available space between what has been made possible by AI and what is permitted by law, in order to discuss what is appropriate". However, also the embodiment of ethically-driven solutions in the design ("ethics-by-design") is a recommended method of practical implementation.

It is possible to extract five core principles:

- Transparency and Auditability. Explicit references are made to the "black box" problem and the need of ensuring explainable AI decisions (p. 114-115), also by means of promoting research (p.118). Explainability is directly linked to the accountability of decisions that have an impact on fundamental rights and freedoms. The document straightforwardly affirms "as a society, we cannot allow certain important decisions to be taken without explanation" (p. 115). Transparency and auditing solutions are then proposed. Regarding the former, it is noted that "businesses that have invested substantial sums of money in the construction of their algorithmic systems and would like to reap their rewards are necessarily reluctant to see their intellectual property divulged to third parties"(p.117); then, a solution in public auditing done by expert commissions is proposed alongside incentives to ensure a wide access to data and algorithms also for the purposes of validating legal and ethical compliance of the systems;

- Fairness. Tackling discrimination seems a major concern (p.113), as "[t]he use of deep learning algorithms, which feed off data for the purposes of personalization and assistance with decision-making, has given rise to the fear that social inequalities are being embedded in decision algorithms" (p.116). For these purposes, an *ex-ante* "Discrimination Impact Assessment" is proposed as a self-evaluation intended to prevent unfair outcomes of AI systems deployment.

- Accountability and Explainability (as research areas). The responsibility correlated to the use of machine learning systems is defined as a "a real scientific challenge" due to the necessary balance that has to be found between the necessity of explaining automated decisions and the efficiency of algorithms used to make them. In fact, while some algorithms are more explainable - yet, less precise - than others (p. 115), the social acceptance of certain automated decisions might be low if no justification is provided. Therefore, research into accountability and explainability is recommended (p. 118);

- Privacy and (group) data protection. One of the most innovative and perhaps controversial fields of the Villani Report is the provision of collective rights to data. First, the importance of aggregated data for AI is juxtaposed to the "blind spots" of EU and French data protection law. As aggregated data fall outside the scope of data protection law (as far data are no longer referred to identified or identifiable individuals), the collective dimension of the effects of decisions on groups is left unprotected (p. 121). A possible solution is found in the implementation of collective or class actions supported by compensation for injuries (p.122);

- Inclusiveness. Given the importance of the ethical questions at stake, an inclusive debate is recommended. Following the German Data Ethics Commission, a national advisory committee is proposed as a *forum* for coordinating such ethical discussion (p. 128) by mediating the positions of the industry, institutions, NGOs, academia, trade unions, etc. Institutional and public consultations via surveys and opinion polls would fall within the competences of this committee (p. 129).

SIGAI, The Special Interest Group of AI: "Dutch AI Manifesto" (SIGAI, 2019)

The Dutch Artificial Intelligence Manifesto originates from academic researchers operating in the area of AI. The technical sections of the document reflects its nature by discussing cutting-edge AI applications, including machine learning. Despite not presenting an explicit list of principles, some morally-relevant *desiderata* can be retrieved from some passages.

- Fairness. This goal is briefly mentioned when discussing the trade-off between algorithmic efficiency of reinforcement learning algorithms (p. 12). Fairness seems related to the social awareness of AI, i.e. its capability of integrating and interacting with human-populated environments. As a consequence, machine learning systems should not provoke negative effects on individuals when analysing human behaviour, group interaction patterns, and emotions. This dimension is included in the Socially-Aware AI paradigm, i.e. the promotion of a collaborative AI that is capable of interacting with humans, interpreting and positively influencing human behaviour while coordinating its interaction with individuals.

- Explainability. As with other documents, Explainability is presented as a challenge that regards the opacity of "black box" algorithms and the effects of automated decisions on individuals (p. 14). On the one hand, research is needed to ensure that available machine learning techniques guarantee a sufficient understanding of their internal structure; on the other hand, users shall be able to interact with the system to grasp the "why and how" the decision has been taken by means of intelligible user interfaces.

- Accountability. Presented within the context of "Responsible AI", accountability refers to the *ex post* validation of the behaviour displayed by an AI system from a moral and legal perspective. Responsible AI mitigates the risks emerging from a wide range of scenarios - from algorithmic biases to privacy-invading technologies - that require the adoption of an ethical aptitude and the respect of normative standards. Accountability is then needed to trust the use of these systems and their convergence towards value-oriented behaviours.

One commentator (Bart, 2020) has underlined the multidisciplinary character of the Dutch AI Manifesto when it comes to the three *desiderata* mentioned above. With this regard, the relationship between social, explainable, responsible AI and the efforts of the legal informatics academic community in promoting AI & Law conferences such as ICAIL and JURIX have been underlined. Other reviewers (Ryan and Stahl, 2020) have underlined the role of Sustainability, a key dimension of environmental social awareness. In this area, a possible limitation of this study might be the acceptance of a possible over-influence of AI systems over humans, especially in light of what has been promoted by other charters as regards the human oversight and prominence over AI systems, a component that is missing in the Dutch Manifesto.

AGID, Agency for Digital Italy : "White Paper on Artificial Intelligence at the service of the citizen" (AGID, 2018)

The Italian AI strategy has been preliminary drafted by the "White Paper on Artificial Intelligence at the service of the citizen" released by a task force within the National Agency for Digital Italy (AGID, 2018). The document mainly pertains to the adoption of AI systems by public institutions and its inclusion seems convenient in light of the scope of our analysis. Ethics and principles are identified among the "Challenges at the service of citizens" and are displayed on top of the list. Principles endorsed by the document represent a convergent positions between the AI "enthusiasts", i.e. those who propose a straightforward adoption of AI systems at all level with no conditions, and "doom-mongers", i.e. those who sceptically reject the integration of AI systems within public administrations due to possible threats to individuals' rights and freedoms.

Four elements of debate and *desiderata* are presented as a way to commit to an adoption of AI systems for the public sector that is beneficial for the general public.

- Data quality and neutrality. This principle correlates to a fair construction of datasets, in particular to avoid the introduction or the replication of errors and biases that might open the room for discrimination (ethnic differences in crime prevention AI systems are mentioned). The over/underestimation of the weight of certain variables is likely to raise issues regarding the interpretation of machine-generated previsions. Non-discrimination is also discussed in Challenge 7 "Preventing Inequalities", which suggests a proactive approach for which AI systems should minimise the existing differences rather than allowing their increase.

- Responsibility (accountability and liability). This principle covers both the legal liability for the use of AI systems by public bodies, but also the moral dimension of accountability. Some of the issues discussed "highlight the need to establish principles for the use of AI technologies in a public context" and the political responsibility of AI-supported decisions.

- Transparency (and Openness)[218]. These principles are "fundamental prerequisite" for a trustworthy adoption of AI systems by public decision-makers in light of the objective of avoiding discrimination and information asymmetries. Therefore, transparency is needed to guarantee citizens' right to understand public decisions. It is remarked that algorithms could introduce social discrimination. However, explicit recommendations (e.g. explainability, auditing, disclosures) are missing and it is fairly hard to grasp the essential meaning of transparency for the purposes of this document.

- Protection of the private sphere. While this principle seems broader that data protection as it might refer to non-informational dimensions of privacy, the discussion that follows is mainly focused on the protection of personal data. In particular, public bodies should commit themselves to protect citizens' data, in particular those sensitive, and when data are used in contexts other than the original one for which they have been collected.

[218] As no further references of "openness" are provided in the document, I would cautiously assume that the term is used *ad abundantiam* to support transparency. As such, the two terms are used as synonyms

Due to its limited scope, namely the deployment of AI in public administration, the advantage and the main drawback of the Italian AI strategy consists of its narrow remit. On the one hand, it contributes to enrich the institutional perspective by analysing *desiderata* of public bodies. On the other, it lacks of the generalisability/universality that marks other Charters.

On July 2020, the Italian AI strategy was enriched and finalised by an other document[219] listing several policy recommendation. While maintaining the human-centric premises of the previous version, this new document highlights the necessity of collaborating to the debate on AI Trustworthiness (p. 24) and recommends the Government to carefully align with to the EU AI ethics vision and its human-centric approach (p. 87).

4.2.2 Interdisciplinary ethical charters

Auxiliary sources consist of documents that have been drafted and released in non-institutional contexts, namely a multi-stakeholder forum (Asilomar Conference), an engineering and informatics non-profit organisation (the Institute of Electrical and Electronics Engineers (IEEE)), an academic-driven group (AI4People) and the HLEG set out by the EU Commission. These document will be used as additional resources to identify the origins of the aforementioned institutional charters and to approach the current debate on AI governance from a broader perspective.

Asilomar Conference (Future of Life Institute, 2017)

The Future of Life Institute 2017 Beneficial AI Conference, also known as Asilomar Conference, is one of the first modern examples of international and multi-stakeholder[220] discussion on AI ethics. Following a 2.5 days debate, the Conference produced a list of principles as its outcome. The list has been drafted starting from existing reports released by academic, governmental, industrial and non-profit entities. Simplifications, summaries and surveys, both at individual and group level, were then carried out. Finally, the list of 23 principles on which a 90% agreement had been reached was adopted.

[219] To date (August 2020), the English translation of the document is not yet available. The original version is available at https://www.mise.gov.it/images/stories/documenti/Proposte_per_una_Strategia_italiana_AI.pdf

[220] To date (October 2020), Asilomar Principles have been signed by 1668 AI/Robotics researchers and 3654 other signatories

Focusing on principles 6 to 18 ("Ethics and Values"), it is possible to cluster them into some groups:

- Beneficence. Principle 14 ("Shared Benefit") and 15 ("Shared Prosperity") promote the collective benefit of AI development;

- Accountability. Principle 9 ("Responsibility") calls for moral thinking to be requested to AI developers and designers regarding the use and misuse of AI technologies. Then, Principle 10 ("Value Alignment") sets the direction for moral thinking by requiring that AI is designed to operate according to human values;

- Transparency. Principle 7 ("Failure Transparency") and 8 ("Judicial Transparency") specify that it is necessary to design systems that are transparent when failing and provide explanations when operating. However, the second transparency measure is limited to AI systems deployed in the context of judicial decision-making;

- Security. Principle 6 ("Safety") requires that AI systems are safe and secure when operating. No further specifications are offered as regards the nature of such safety (e.g. data, physical infrastructure, non-discrimination). Principle 7 ("Failure Transparency") completes the principle of Safety with an *ex-post* perspective on the necessity of preserving the possibility of scrutinising the reasons for mistakes;

- Control. Taken together, principles 10 ("Value Alignment"), 16 ("Human Control"), 17 ("Non-subversion"), 18 ("AI Arms Race") strongly encourage the development of AI systems that can ensure human oversight from different perspectives, all united by ensuring the promotion of human values. Firstly, humans should be free to rely or not on AI systems for decision-making processes; secondly, AI should not threaten human health; thirdly, AI arms race should be avoided;

- Privacy. Principles 12 ("Personal Privacy") and 13 ("Liberty and Privacy") reflect the threats to personal data and individual rights and freedoms that rise when discussing the implications of AI systems. While the former principle is mostly focused on giving the right to "access, manage and control" personal data, the latter takes the broader perspective of protecting individuals' "real or perceived liberty".

IEEE Ethically Aligned Design (IEEE, 2017)

Within the context of IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, IEEE has published two versions of "Ethically Aligned Design" in 2016 and 2017[221], aiming at establishing "ethical and social implementations for intelligent and autonomous systems and technologies, aligning them to defined values and ethical principles that prioritize human well-being in a given cultural context." (p. 2). The document purposively covers a wide range of AI technologies and analyses their ethical implications from the viewpoint of researchers, manufacturers, and designers of intelligent and autonomous systems, with specific focuses on lethal autonomous weapon systems and "strong" AI applications.

An explicit list of five principles is then identified:

- Human Rights. AI should respect internationally recognised human rights enshrined by the Declaration of Human Rights, UN treaties and international conventions. Fundamental rights and freedoms shall be preserved in any AI application. This entails the preservation of safety in the runtime of the system and the traceability of possible failures;

- Well-being. Crucially, IEEE points out that there are no established metrics of well-being, hence the possible failure of attempts made to promote it in the development of AI applications. Therefore, the promotion of well-being has to be contextualised to certain metrics, even beyond Gross Domestic Product (GDP);

- Accountability. As with other charters, IEEE also focuses on the necessity of holding some entities responsible for the harms caused by intelligent and autonomous systems. Since no specific entity can be found *a priori* liable, a distributed form of apportion culpability among manufacturers (which carry the burden to prove the correct functioning of the system), designers, operators, owners. This is deemed necessary to ensure a trustworthy and widespread adoption of AI systems;

- Transparency. This principle ensures that "it is possible to discover how and why a system made a particular decision, or in the case of a robot, acted the way it did". The principle of Transparency has three nuances: traceability, explainability, and interpretability. These facets are needed to understand what the is system is doing, validate and certificate AI systems, investigate mal-

[221] In our analysis, we will refer to the Version 2 of the document, available at https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead_v2.pdf

functioning, carry out legal investigations, increase trust towards AI systems (in particular, disruptive technologies);

- Awareness of Misuse. AI designers and programmers, citizens, and decision-makers should be educated towards a responsible use of AI systems focused on the development of accountability mechanisms.

AI4People initiative (Floridi, Cowls, et al., 2018)

The promotion of a "Good AI Society" is the foundational scope of an other international initiative, AI4People within the Atomium-EISMD consortium. The article first discusses opportunities and risks of AI with a focus on human dignity; then, it identifies five principles that should steer AI development and deployment; finally, it elaborates 20 principle-based recommendations that could promote a responsible adoption of AI systems.

Methodologically speaking, the AI4People initiative identifies ethical principles taking inspiration from bioethics[222] and previous works done in the context of AI ethics.

- Beneficence. Taking inspiration from previous works in AI ethics, AI4People authors synthesise existing principles as the need of creating AI technologies are beneficial for humanities and promote the "well-being of people and the planet";

- Non-maleficence. This principle calls for the avoidance of negative consequences linked to the misuse of AI systems. Risks might emerge in the field of privacy and data protection, arms race (as already pointed out by the Asilomar Principles), or in other sectors discussed in other ethical documents. In AI4People, the principle of non-maleficence as harm prevention encompasses both accidental and deliberate harms, respectively referred to as "overuse" and "misuse". Moreover, both human (e.g. developer) and machine behaviours are subject to this principle;

- Autonomy. AI4People authors found large consensus on ensuring the freedom to choose to rely on human or automated decision-making processes. Interestingly, they propose a "static" perspective, which promotes the prominence of human autonomy, and a "dynamic" perspective, according to which

[222] As the authors state: "Of all areas of applied ethics, bioethics is the one that most closely resembles digital ethics in dealing ecologically with new forms of agents, patients, and environments". The conclusion was previously reached by Floridi (Floridi, 2013a)

the autonomy of machines should be made "intrinsically reversible" and human subversion shall be guaranteed following an initial delegation to AI. Individuals should also be free to choose whether or not to rely on AI systems ("meta-autonomy") for reasons overriding efficacy;

- Justice. In works previous to AI4People, the social implications of AI are discussed under several dimensions, including a proactive aptitude to reduce discriminations, sharing benefits of the adoption of AI technologies, preventing unknown harms. By acknowledging these dimensions consistently with their bioethical approach, AI4People authors identifies "justice" as the need of ensuring that AI-related resources and benefits are distributed widely;

- Explicability. Differently from other principles, explicability is not derived from bioethics. It specifically relates to AI and constitutes one of the most prominent elements of novelty in AI4People research. Previous works used different terms to express the ability to understand AI systems inner logic ("transparency") and to identify the responsible entity ("accountability") for the use of these technologies. In addition to them, AI4People authors conceptualise Explicability both in the epistemological sense ("intelligibility", or the making sense of the operations performed by AI systems) and in the ethical one ("accountability", or the identification of a responsible entity for the work done by the AI).

EU Commission High Level Expert Group: "Guidelines for Trustworthy AI" (HLEG, 2019)

The EU Commission High Level Expert Group (HLEG) is one of the most discussed institutional initiatives on AI Ethics[223]. Its Guidelines for Trustworthy AI set out a framework for achieving a lawful, ethical and robust AI systems' life-cycle. Therefore, as the authors state, their outcome aims to go "beyond a list of ethical principles" (p.2). Such framework consists of three essential components: four ethical principles, seven key requirements, and an assessment list to verify adherence to principles and requirements.

Ethical principles (in yellow), key requirements (in green) and their details (in orange) are displayed in the picture below. Ethical principles are based on fundamental rights enshrined in the EU Treaties, the Charter and international right law (p. 9). The consist of:

[223] The Expert Group was set up by the EU Commission in June 2018. As stated in the foreword, the content of the document does not reflect the official position of the Commission, hence the inclusion among our auxiliary sources

- Respect for human autonomy. This principle mirrors human dignity and the right to self-determination and prescribes that, when using AI systems, humans shall not be manipulated or deceived by the system. When developing AI technologies, such human-centric approach shall be ensured by securing human oversight, i.e. the ability to control the system by various degrees[224];

- Prevention of harm. AI may cause or exacerbate harms to human dignity or physical or bodily integrity. Therefore, it is necessary to mitigate threats to human beings by ensuring that AI systems are secure and resilient. This principle consists of several dimensions which range from the protection of data integrity (including personal data protection), quality and accuracy. In particular, the HLEG recommends to keep into account vulnerable people, situations of informational asymmetries and natural environment when identifying risks to mitigate;

- Fairness. This principle has a substantive and a procedural dimension. From the substantial perspective, fairness implies a) that unfair and discriminatory AI-supported decisions shall be avoided, and b) that proportionality between means and ends in the use of AI systems is kept into account by AI practitioners. From a procedural perspective, Fairness shall grant the possibility to seek redress for the automated decisions made by AI algorithms, accountability mechanisms for the use of AI systems and explicability of AI decisions;

- Explicability. Juxtaposed with "black box" algorithms, this principle pertains to the design of AI systems capable of communicating their processes and their output, also in relation to the context of deployment and the risks generated by the outcomes. Explicability is needed for a plethora of reasons: to promote trust in AI systems, to contest AI-supported decisions, to verify compliance with fundamental rights.

[224] The HLEG discusses three alternatives (p. 16): human-in-the-loop (HITL), human-on-the-loop (HOTL), and human-in-command (HIC). HITL refers to the capability of controlling every operation of the system for an human; HOTL is the ability to control the design of the operations (*ex ante*) and monitor them (*ex post*). HIC is the ability to scrutinise and possibly steer the large-scale effects of the systems, including societal ones

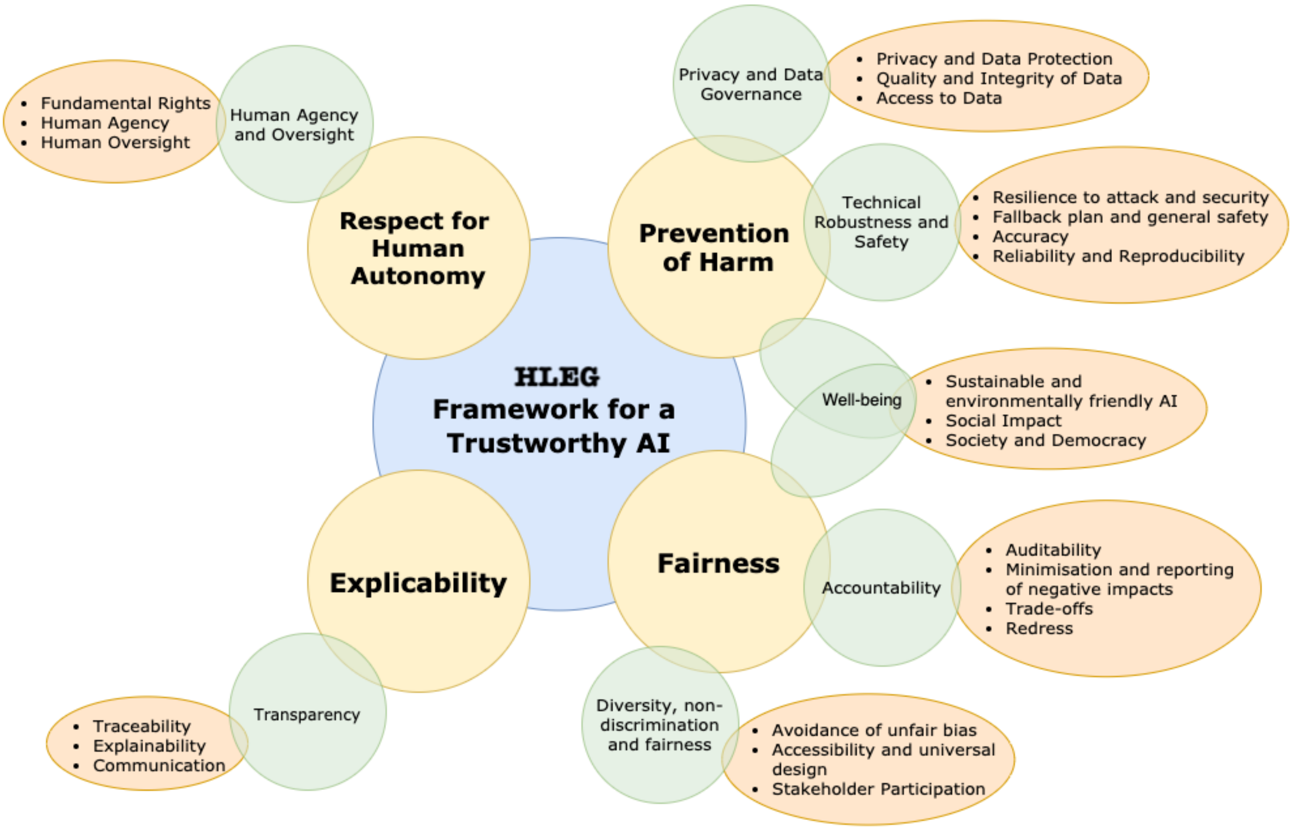

Fundamental Rights
Human Agency
Human Oversight
Human Agency and Oversight
Respect for Human Autonomy
Privacy and Data Governance
Privacy and Data Protection
Quality and Integrity of Data
Access to Data
Prevention of Harm
Technical Robustness and Safety
Resilience to attack and security
Fallback plan and general safety
Accuracy
Reliability and Reproducibility
HLEG Framework for a Trustworthy AI
Well-being
Sustainable and environmentally friendly AI
Social Impact
Society and Democracy
Explicability
Fairness
Accountability
Auditability
Minimisation and reporting of negative impacts
Trade-offs
Redress
Transparency
Traceability
Explainability
Communication
Diversity, non-discrimination and fairness
Avoidance of unfair bias
Accessibility and universal design
Stakeholder Participation

Figure 4.1: EU Commission HLEG on AI - Key Findings

The work done by the HLEG has been criticised by one of its members - Thomas Metzinger - because of the group's composition, allegedly too unbalanced towards non-ethicists (48 vs 4 ethicists) and its proximity to the industry which was reflected in censorship[225]. These claims are undoubtedly out the scope of this dissertation and we will leave them to scholars more interested in gossip than advancements of academic debate[226]. As regards their contents, the Guidelines have been defined as "lukewarm, short-sighted and deliberately vague" and, at the same time, "the best globally available platform for the next phase of discussion" by Metzinger. Other scholars have criticised the absence of certain rights and freedoms (e.g. the freedom

[225] Metzinger's claims were made by means of an article at Der Tagesspiegel available at https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html

[226] However, it is worth reminding that the decision-making process of the HLEG was open to public feedbacks, available at https://ec.europa.eu/digital-stiingle-market/en/news/over-500-comments-received-draft-ethical-guidelines-trustworthy-artificial-intelligence: more than 500 comments were received over the first draft and significant changes were made before the final publication

to assembly) and the appearance of topics placed outside EU Charters and Treaties, e.g. sustainability (Wagner, 2018).

4.3 Data and AI Governance: methodological pitfalls and proposed solutions

Following the description of our sources, some critical remarks have to be discussed. This section aims to first identify some methodological limitations of AI charters and, from a broader perspective, some of the risks linked to the idea of an AI ethics at discussed within the current debate. We will refer to the five threats identified by Floridi (Floridi, 2019b), namely ethics shopping, ethics bluewashing[227], ethics lobbying[228], ethics dumping[229], and ethics shirking[230].

Defined as "the malpractice of choosing, adapting, or revising (mixing and matching) ethical principles, guidelines, codes, frameworks, or other similar standards (especially but not only in the ethics of AI), from a variety of available offers, in order to retrofit some pre-existing behaviours (choices, processes, strategies, etc.), and hence justify them a posteriori, instead of implementing or improving new behaviours by benchmarking them against public, ethical standards", "ethics shopping" is certainly the only foreseeable risk of our Roadmap among the ones identified by Floridi due to the inclusion of multiple principles and guidelines to draft our ethics-based Roadmap. Rather than relying an *a posteriori* justification, *a priori* inclusion criteria for selected principles will be presented at the end of this section. Beforehand, it is also necessary to discuss some other limitations of AI ethics and AI charters.

[227] "Ethics Bluewashing" is defined as "the malpractice of making unsubstantiated or misleading claims about, or implementing superficial measures in favour of, the ethical values and benefits of digital processes, products, services, or other solutions in order to appear more digitally ethical than one is". Color blue is to differentiate Bluewashing from "Ethics Greenwahsing", that is the malpractice of appearing more environmental-friendly or sustainable than the actuality of things

[228] "Ethics Lobbying" is defined as "the malpractice of exploiting digital ethics to delay, revise, replace, or avoid good and necessary legislation (or its enforcement) about the design, development, and deployment of digital processes, products, services, or other solutions"

[229] "Ethics Dumping" is defined as "the malpractice of (a) exporting research activities about digital processes, products, services, or other solutions, in other contexts or places (e.g. by European organisations outside the EU) in ways that would be ethically unacceptable in the context or place of origin and (b) importing the outcomes of such unethical research activities."

[230] "Ethics Shrinking" is defined as "the malpractice of doing increasingly less ethical work (such as fulfilling duties, respecting rights, and honouring commitments) in a given context the lower the return of such ethical work in that context is mistakenly perceived to be"

Then, by using the methodology of the middle-out layer of analysis (Pagallo et al., 2019), we will define an interface for our data governance model. Rather than making explicit *which* model should be implemented among the possible policy options, this subsection will identify "Trust" as the interface needed to develop data governance frameworks in the domain at stake. To this end, our Roadmap constitutes a principle-based implementation of any current or future data governance framework based on trust and applicable to agri-food safety risk assessment.

Finally, we set methodological constraints to prevent ethics shopping. In particular, inclusion/exclusion criteria for candidate principles are derived from the existence of consensus among institutional charters on well-established principles, adherence to the existing legal framework and pertinence to the technical evidence shown in previous Chapters.

4.3.1 Methodological limitations of AI Charters

The involvement of the industry in AI Ethics debate

Private companies have been active in the field of AI Ethics. Most of their efforts have been steered towards the release of documents drafted to resemble "AI Ethics manifestos", often following the appointment of one or more philosophers (Bietti, 2020), or by taking part directly or indirectly to discussions in existing working groups, as already noted e.g. in the case of Asilomar Conference and the EU Commission HLEG. Since commercial entities constitute a significant portion of EFSA's stakeholders and of the domain of food safety risk assessment in general, it is worth discussing the extent to which their involvement in AI Ethics discourse can be problematic and what solutions will be proposed by this dissertation.

Morley (Morley, Floridi, et al., 2019) has noted that industrial conglomerates such as Google, IBM, Microsoft, Intel have released their own Charters. The proliferation of company-driven initiatives has also been observed by other reviewers (Fjeld et al., 2020; Jobin et al., 2019). However, these efforts have not been unanimously welcomed by scholars in the field of law and ethics, who have refereed to this trend as "ethics washing" - i.e. a trend described as the use of "ethics" language intended to prevent legislative actions by imposing principle-based forms of self-regulation, while making AI practices palatable for the public (Calo, 2017, p.408) (Wagner, 2018) - that resembles Floridi's "Ethics Bluewashing" and "Ethics Lobbying" together. Moreover, findings from internal ethics boards seem to lack of any positive effect on individuals and society as a whole for being selfishly produced by private entities only to preserve their reputation; then, they might lack of intrinsic and justice value for being carried out in bad faith and, even if they were pursued in good faith, they would raise epistemic issues related to the chance that findings "reinforce a narrow and confined vision of the possibilities of regulatory change, and inhibit dialogue." (Bietti, 2020).

As regards the first set of critiques, in 2018 the Commission declared that "[w]hile self-regulation can provide a first set of benchmarks against which emerging applications and outcomes can be assessed, public authorities must ensure that the regulatory frameworks for developing and using AI technologies are in line with these values and fundamental rights. The Commission will monitor developments and, if necessary, review existing legal frameworks to better adapt them to specific challenges, in particular to ensure the respect of the Union's basic values and fundamental rights."[231]. This clarifies the scope of this (allegedly) pre-emptive self-regulatory attempt performed by AI-supporting companies: the perspective offered by institutional decision-makers seems to be resistant to the pressure to let key sectors self-regulated. The premises of the second critique seem acceptable if we consider the promotional nature of company AI manifestos. Nonetheless, brand reputation and trust might still constitute a sufficient incentive to observe principles to which the company is committing. If "ethics washing" is synonymous with "advertising", then consumers might have legitimate expectations of compliance[232]. Incidents and failures, insofar they can be linked to a malicious non-compliance of self-imposed principles, would result in financial loss and distrust among consumers. As regards the third critique, it is simply not possible to determine *ex-ante* whether or not private AI initiatives prevent institutional scrutiny over private actions, and regulatory models such as the GDPR[233] seem to prove the contrary.

In light of our methodology, other critiques may be decisive in defining our approach towards company-originated documents. On the one hand, the aforementioned companies operate internationally and their charters have to reflect the global nature of AI problems across different legal frameworks. The scope of this dissertation, instead, is explicitly EU-centric and shall therefore mirror the principles enshrined in the EU treaties and legislation. On the other hand, certain documents cover specific market sectors (e.g. autonomous vehicles) and, to date (October 2020), no food-safety relevant guideline has been released. Since the inclusion of company-originated documents may constitute an unnecessary source of uncertainty in our results, these types of documents have not be taken into account.

[231] https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe, p. 7

[232] In the different context of social media platforms and search engines, Balkin (Balkin, 2017, p.1183) has observed when digital platforms become *information fiduciary* by building trust-based relationship with their end users, they might have expectations of care and regulation towards private companies since they were subject to codes of behaviours. *Mutatis mutandis*, self-imposed and ethics-based non-mandatory code of conducts might have similar effects

[233] In particular, the GDPR provides for self-regulatory mechanisms, such as certifications, data protection seals and marks (art. 42). However, the existence of these mechanisms does not exclude the responsibility of data controllers and processors for compliance with the Regulation (Art. 42.2)

The question of Trustworthiness

In his letter mentioned above, HLEG member Thomas Metzinger argued that "[t]he Trustworthy AI story is a marketing narrative invented by industry [...]. The underlying guiding idea of a “trustworthy AI” is, first and foremost, conceptual nonsense". He also pointed out that "[m]achines are not trustworthy; only humans can be trustworthy (or untrustworthy)" and claimed that trustworthiness is part of a marketing strategy.

Metzinger’s second claim does not seem confirmed by reviewers (Smit et al., 2020) that observed that "Trustworthy AI[234]" appears more frequently in "AI charters" released by non-profit entities (22%) than in documents produced by for-profit undertakings (17%) (figure 4, n = 30). However, their findings show that trustworthiness is largely overlooked in AI Charters, as only a relatively small fraction of AI guidelines mentions AI trust among their goals[235].

Metzinger’s first claim on AI trustworthiness seems far from the approach taken by other scholars. *Inter alia*, Taddeo (Taddeo, 2017) correctly illustrates the role of trust in delegation to machine learning softwares by stating that "as digital technologies evolve and become more refined and effective, our expectation has become an expectation to trust (by delegating and not supervising) them with important tasks". However, trust in machine learning (specifically) and AI systems (in general) shall not entail complete autonomy of the system and loss of human control ("trust and forget" approach)[236].

Our findings in §2.5 seem to accept these two positions. We discussed the phenomenon of *delegating delegations* in terms of a two-orders relationship. On the one hand, individuals delegate the entities involved in risk assessment authorities to duly verify the level of safety of foods. On the other hand, these entities delegate the "hard taks" of risk assessment - those which deal with the analysis of large quantities of data - to machine learning algorithms. For the first order of delegation (citizen → entity), it is true that can only be trust in the users of AI systems alone rather than towards algorithms and softwares. For the second order of delegation (entity → AI system), trustworthiness is the expectation of delegating without supervising.

Not only can different positions on trustworthiness be contextually approached in

[234] Smit and colleagues (Smit et al., 2020) defined trustworthiness design principle as "[a]n AI must be designed and used so that it’s deserving of trust, or able to be trusted"

[235] In some cases, however, trust is the goal towards other principles aims (e.g. (IEEE, 2017, p.29-30)) and it is unclear whether or not reviewers included such implicit references in their count

[236] Let us consider the case of Microsoft chatbot Tay, which was left operational for 16 hours while it acquired offensive language by interacting with users on Twitter. Before being shut down, Tay published 96.000 tweets

our domain, but also the centrality of trust in the allocation of data ownership rights while inspiring openness and transparency measures has to be remarked (§3.4.1). Therefore, despite the poor attention given by AI Charters other than the HLEG and few others, it seems convenient to include trust and trustworthiness of AI *users* and *systems* in the forthcoming analysis.

The relationship with bioethics

A certain degree of convergence around the four bioethical principles of Benefice, Non-Maleficence, Autonomy and Justice (Beauchamp, Childress, et al., 2001) can be found in the conceptual framework adopted by AI4People, which first found agreement among previous sources (including the Asilomar AI Principles and IEEE initiative mentioned above). In accordance with this position, bioethics is consistent with the onto-centric, patient-oriented, ecological premises of information ethics (Floridi, 2013a, ch.4.5). In turn, it has been endorsed by the HLEG and consequently taken into account by the EU Commission's White Paper[237].

Mittelstadt (Mittelstadt, 2019) has welcomed the adoption of medical ethics principles by claiming its convenience "as it is historically the most prominent and well-studied approach to applied ethics". Advantages consist of an inclusive discourse that keeps into account the needs of all the actors involved, some degree of flexibility when contextual-dependent balances are needed, and the capability of framing ethical challenges and provide clinical decision-making guidance. AI ethics seems intended to add some kind of normative content addressed to decision-makers and AI designers.

However, other commenters (Renda et al., 2019, p.47) underlined the inadequacy of bioethical approach, as "principles of bioethics can impose excessive burdens on AI systems if applied without paying heed to the principle of proportionality or giving guidance on how principles will be endorsed or enforced". While recognising the necessity of setting directions on how these principles will be respected and the key role of proportionality, this position does not clarify how such burdens would be imposed to AI systems and their nature (e.g. administrative, financial, and so on). Rather, it seems plausible that such obligations would be placed on AI developers or end-users rather than on the system.

In light of our findings presented in the previous subsection regarding trustworthi-

[237] Noteworthily, the OECD has shared the bioethical perspectice in the document "Recommendation of the Council on Artificial Intelligence" (not included among our sources) available at https://www.oecd.org/science/forty-two-countries-adopt-new-oecd-principles-on-artificial-intelligence.htm

ness, bioethical principles seem appropriate to impose fiduciary obligations on developers when designing AI systems and end-users when operating them. This finding has been reached in trust-dependent contexts, such as healthcare (Nabi, 2018). It has been noted (Mittelstadt, 2019) that, in the absence of a regulatory framework creating such fiduciary relationship, personal convictions of developers or other factors might be insufficient in ensuring that bioethical (and ethical) principles would be translated into practice.

Such limitation, however, affects our context only partly: the novel introduction of the Transparency Regulation is explicitly intended to promote fiduciary relationships between all the entities involved in data collection and analysis, according to the model presented in the previous Chapter. Therefore, since an existing regulatory framework is meant to foster trust among all the actors involved, bioethical principles represent a safe way to steer the modelling of our Roadmap[238].

The technological neutrality

A methodological limitation, not yet fully discussed by the literature, regards the technological neutrality of AI charters. This expression might sound rather ambiguous, antinomic or even nonsense, hence the necessity of clarifying it. In general, technological neutrality entails that the same principles, legal or regulatory framework shall apply indistinctly to all the technologies that fall within the scope of the normative instrument[239].

Despite being related to a "technology", AI charters that constitute our sources share the same view. Apart from specific case studies, they do not specifically consider AI approaches (e.g. supervised/unsupervised learning), algorithms (e.g. neutral networks, regressions), or applications (e.g. facial recognition, robotics) when listing principles or describing their implications. Here lies the technological neutrality of AI guidelines.

For the purposes of verifying the adequacy of AI charters to a given domain, it might be necessary to contextualise their guidelines to the technical peculiarities that such domain presents, e.g. the nature of data analysed by AI systems, the kind of bias

[238] This does not entail, however, that principle-based normative implementations would not be needed. See more at §5.3

[239] For instance, in copyright law, the definition of communication to the public is said to be technologically neutral for being independent of the means of communication (e.g. VOIP, social media, wireless, wired broadcasting, and so on) (Aplin, 2020, p.221). Recital 15 of the GDPR is more explicit on the point, as it states that "[t]he protection of natural persons should be technologically neutral and should not depend on the techniques used" to prevent risks of circumvention

that might emerge from their analysis and the design solutions adopted in a given context that might prevent discriminations. This does not necessarily translate into a mere "ethics-by-design" approach that aims to solve ethical questions by framing them into design or engineering problems. Instead, this approach aims to adapt high-level principles to a specific technical domain (top-down). In turn, it validates the same high-level principles by discussing their implications in domains largely overlooked by academic discussion and policy-making. These new areas may serve as a test for the resilience of cross-sectoral AI charters (bottom-up).

The technical review proposed in Chapter 2 fulfils the necessity of understanding the technical domain of AI to certain approaches that emerge in our context. Therefore, we will use findings presented before to draft principle-based solutions that are suitable to the peculiarities of the domain at stake while being consistent with general conclusions regarding AI.

4.3.2 Between top-down and bottom-up data governance: the middle-out layer analysis

So far, we have identified certain methodological weaknesses of AI charters and try to advance solutions that should guarantee a certain degree of consistency between high-level principles, domain-specific regulatory frameworks and technical advancements. This section identifies how this balance is plugged into the discourse on data governance.

Pagallo and colleagues (Pagallo et al., 2019) have introduced the concepts of "middle-out layer" and "middle-out approach" to the debate on data, AI and web of data governance. Their investigation looks for "what lies in between" top-down and bottom-up approaches to legal governance. Traditional models consists of "top-down" (e.g. enforced regulation), and "bottom-up" (e.g. self-regulation). Authors' methodology aims to verify the extent to which the convergence between multiple regulatory systems - which include primary and secondary rules - strikes a balance between technology, market and social norms.

The Authors have adopted their approach when discussing *de iure condito* the GDPR and the principle of accountability, which was found to be GDPR's middle-out interface aiming to minimise risks related to data processing. In their view, Accountability lies in between GDPR principles and rules, on the one hand, and organisational and technical (*by-design* and *by-default*) measures, on the other. As regards AI regulation, Pagallo and colleagues have identified coordination mechanisms as the middle-out layer between "no-regrets" actions on which a significant degree of consensus has been shown by EU Commission and the engagement of AI industries and AI-enhanced market sectors.

By breaking down these components, it emerges that the identification of a middle-out layer of analysis is methodologically convenient for our domain.

First, this approach aims to strike a balance by multiple regulatory systems, consisting of primary and secondary rules (Hart, 1961). As the normative discussion proposed in Chapter 3 has highlighted, several pieces of legislation concur to define the legal framework of interest: a general regulation (the GFLR), sectoral legislation, and other provisions that relate to specific portions of the data processing activities at stake (e.g. the processing of personal data and the GDPR). Consistently with our data-centric approach, the middle-out layer analysis should be focused on data-related provisions. Moreover, as the Authors remark, "the law is not the only regulatory system out there": market practices, social values and principles and even technology (Lessig, 2009) shall be conceived as regulatory systems.

Secondly, the middle-out approach investigates how to align primary and secondary rules of the law. In our domain, normative implementations are left to EFSA's discretion when governing data from a legal (e.g. EFSA's confidentiality claims handling) or technical (e.g. data standardisation, additional data requirements) perspective. The middle-out layer of analysis allows us to identify at least a common denominator among these vertical normative sources when applied to the domain at stake.

Thirdly and most crucially, this approach seeks to coordinate bottom-up and top-down regulatory options. As regards the latter, market practices, principles and technology can govern human behaviour and possibly be translated into policy choices. The middle-out layer approach allows us to understand their relationship in our domain. For instance, we noted how principles of openness and transparency are embedded into the system and reflected into the new transparency measures endorsed by the amendments to the GFLR.

One possible outcome of a middle-out layer analysis of our domain, consistently with findings in Chapter 3 and previous discussion, reveals that trust is a cross-sectoral principle that suits the whole EU food safety legislation, the relationship between primary and secondary rules, and competitive regulatory systems. Alongside our considerations in §3.4.1, it is worth mentioning that the lack of trust highlighted by the Fitness Check was across the whole food safety system and all the stakeholders involved, hence the need of reformulating general and sectoral legislation together with primary and secondary rules. As regards market practices, a significant change towards trust can be observed by the committent of the European Crop Protection Association as regards data transparency[240]. Discussing whether or not this is an attempt to escape from more stringent regulations will be left out

[240] https://www.ecpa.eu/industry-data-transparency

from the scope of this dissertation. Either way, this committent seems aligned with the trust-based premises of the new Regulation.

To this end, our Roadmap constitutes one of the many possible implementations of any data governance framework applicable to the domain of agri-food safety that is based on promoting trust, thus including the Transparency Regulation and the complementary legislation. In doing so, it is agnostic to the nature of the regulatory model (regulation, self-regulation, co-regulation, etc.) while preserving the necessary flexibility to be implemented in any policy option.

4.3.3 Contextualising AI principles to food safety Big Data practices and machine learning techniques

Considering some of the methodological limitations highlighted above and the perils of "ethics shopping" already described, it is necessary to refine the selection methodology by setting constraints on the principles that will be added in the Roadmap presented in the next Chapter.

First, only those principles on which a significant degree of consensus has been reached can qualify as candidates. This is similar to the methodological premises of AI4People initiatives and review-based academic papers. This first inclusion/exclusion criterion is needed to ensure consistency between our Roadmap and high-level AI Charters. The references to multiple sources can be detrimental due to an excessive enlargement of principles to be followed, which might trigger conflicts among them as a consequence. Therefore, the first evaluation will aim to identify shared principles.

Second, our analysis is grounded on the existing legislation. One possible approach (Mantelero, 2020) is the one of contextualising principles enshrined in international binding legal instruments to specific areas, also considering the specification of AI products and services, to formulate an initial set of provisions for AI regulation. *Mutatis mutandis*[241], this approach can be refined and adapted to this study. As seen in the previous section, drafting a data governance model that aims to be top-down validated necessarily implies that due consideration is given to the existing legal framework, comprehensive of "hard law" and authoritative interpretations, including case law. For instance, one could argue in favour of a "total transparency" approach that prevents the attribution of ownership rights to commercial entities ac-

[241] As discussed in the Introduction, it is not convenient to rely on the contested human right to safe food the for the purposes of this thesis. Moreover, the international dimension of legal binding instruments is not appropriate to the territorial scope of this document

tive in the field of regulated products. There might be many arguments in favour of this proposal, including the necessity of allowing the cross-validation of scientific data to its largest extent, the existence of an overriding public interest that completely outweighs private interests, the freedom to be informed as a fundamental human right, and so on.

However, none of them would pass the test of resisting to the laws that protect companies' legitimate interest in preserving confidential information. Even without considering the rationale underlying such protection, i.e. fostering innovation by protecting R&D investments, the existence of laws *per se* is the "elephant in the room" that a study grounded on a robust methodology cannot simply ignore unless it positions itself *outside* the existing legislation. While this might be safely done in other research, the proposals advanced by this dissertation are grounded on AI charters that are placed *within* the existing legal framework and aim to interpret and align it rather than radically change consolidated principles.

Finally, the technical domain is the third constraint that we will apply when identifying and selecting principles to prevent "ethics shopping". As already remarked, while this does not necessarily resolve in a generic "ethics-by-design" position, identifying technical boundaries is necessary to better frame the discussion and contextualise high-level principles to the technical domain at stake. Therefore, only those principle which have some connection to large-scale data analysis, including by means of stochastic approaches, will be deemed relevant and, eventually, interpreted in light of their relationship with Big Data and data analysis.

4.4 Chapter Synopsis

This Chapter has illustrated the premises of the "ethical perspective" by justifying the necessity of ethical contributions in the domain at stake, selecting documents following the justification of their inclusion, presenting their contents and discussing some critical remarks advanced by the literature.

In summary, AI institutional charters represent a sound and viable way to identify principles that might be used to interpret and align the existing legal framework of EU agri-food safety risk assessment. Mentioned reviewers have identified a certain degree of consensus among these Charters. A critical appraisal of institutional and complementary sources have provided the knowledge base to select principles to be implemented in the Roadmap presented in the next Chapter.

However, possible methodological limitations prevent an outright adoption of these principles, thus highlighting the necessity of refining their approach in light of the domain at stake. Such domain is identified by the legal framework in place and the technical state-of-the-art. From the combined analysis of these sources, Trust has emerged as the middle-out interface of further analysis and as the ground for the next Chapter, finally discussing the ethical Roadmap which constitutes the main element of novelty of this dissertation. The Roadmap, however, will not commit to a given regulatory implementation (e.g. "hard law") and will leave sufficient room for guaranteeing a smooth translation into any possible regulatory model.

Due to the lack of an explicit reference to a "right to safe food" and the difficulties in framing EFSA's activities exclusively within the frame of the right to health, a principle-based discussion was preferred over the alternative "human right" approach. Moreover, principles derived from bioethics seem appropriate to describe contexts in which trust plays a fundamental role, such as the one at stake.

5

A Principle-Based Roadmap for Food Safety Datafication: The P-SAFETY model

5.1 Objectives and scopes of the Roadmap

In the Introduction (§1.3), a research question was posed: "How can data ownership and data governance be shaped to maximise the benefits and minimise the risks of using a processing Big Data in the context of EU Agri-food safety risk assessment?". This Chapter seeks answers for this question on the basis of the findings emerged from previous Chapters and in light of the methodology adopted so far.

As anticipated, the answer will be given in the form of a Roadmap. Before entering into the details of its contents, it might helpful to clarify the scope and the objectives of the Roadmap, including its relationship with trust.

To briefly restate the methodological premises of the Roadmap, it can be defined as an introductory ethical framework to integrate, interpret and align food safety risk assessment data-related regulatory system to the principles guiding the deployment of AI (*rectius*, machine learning techniques) that have emerged from the policy documents and the academic discussion reported above. On their bases, the Roadmap proposes as a set of general principle-based recommendations to support decision-making processes related to data, algorithms and practices of the domain at stake.

It is possible highlight some features of the Roadmap departing from this concise summary. The Roadmap:

- is an *introductory* framework to be further analysed and implemented. Although some recommendations will be provided throughout the Roadmap, practical implementations will be left to future research;

- is an *ethical* framework since it identifies values and principles that derive from contributions in AI ethics;

- can be used to *integrate, interpret and align* the existing regulatory framework in light AI principles, rather than replacing it. If a "General AI Regulation" will ever come into existence and will be drafted on the basis of the previous works done by the EU Commission, the Roadmap might serve as a trait d'union between food law and the data-related provisions of such hypothetical regulatory framework;

- fosters integration, interpretation and alignment of *data-related* provisions contained in the EU food safety risk assessment regulatory framework. Therefore, its scope is narrower than the one of food safety regulation and mainly concerns risk assessment;

- fosters integration, interpretation and alignment of (mainly) *machine learning techniques* insofar they constitute part of the general notion of AI;

- is grounded on *policy documents and academic literature*. The Roadmap is based on technical, legal and ethical contributions, on the one hand, and EU and Member States AI charters, on the other;

- adopts a *principle-based* approach since it was deemed to be more appropriate than others, including the so-called human rights approach. Noteworthily, principles are indirectly related to bioethics;

- proposes recommendations to *support decision-making processes* at every level, including institutional policy-making or industrial self-regulatory initiatives;

- supports decision-making processes related to *data, algorithms and practices* consistently with the data-centric approach selected as the main technical standpoint.

The Roadmap is trust-oriented. First, it has been noticed (§2.5) that trust is a key element of information collection, analysis and sharing among the entities involved in the food safety system (first-order trust). Then, despite some critiques, the trustworthiness of AI/machine learning systems has been deemed to be a necessary requirement for the delegation of certain risk assessment tasks to algorithms (second-order trust) (§4.3.1). Finally, it is also possible to push further these trust-based relationships and infer the existence of an additional form of trust, i.e. the one that links consumers to AI/machine learning algorithms (third-order trust).

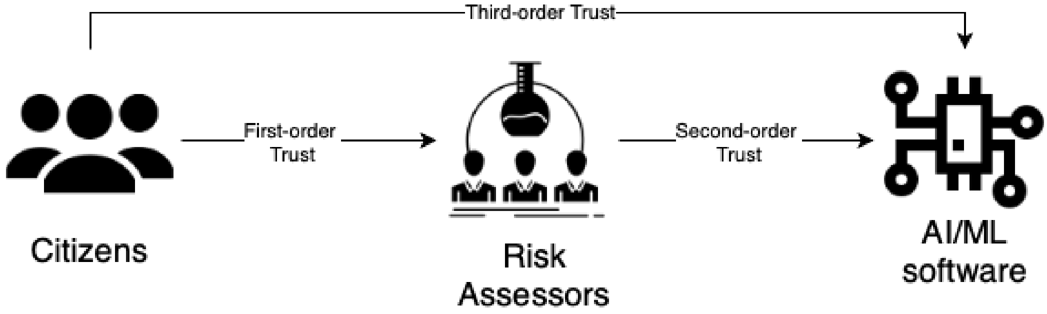


Figure 5.1: First, second and third-order trust. Each arrow represents a Trustor (nock) -Trustee (tip) relationship

While first-order trust is not new, as food safety authorities pre-existed the current datafication process, second-order trust is an emerging phenomenon that correlates with the deployment of machine learning systems. Despite being influenced by the previous two, third-order trust is not merely their sum since it is also linked to the general acceptability of machine learning systems. The Roadmap seeks answer to promote every order of trust.

The proposed list of principles is *non-exhaustive* and *non-hierarchical*. Therefore, other elements might be added in future research, either in light of advancements in legislation or for practical purposes. Moreover, the list shall not be interpreted as a ranking[242] and therefore it is crucial to assume principles enshrined in the Roadmap might conflict either *internally* among them or *externally* with other principles and values, especially in concrete cases and when no *lex superior derogat inferiori* rule could be used[243].When this is the case, one possible unified approach to solve such conflicts might be the Laws of Balancing presented by Alexy (Alexy, 2003)[244],

[242] The nature of privacy as a meta-principle will be clarified in the appropriate sub-section

[243] As in the attribution of weights to the principles in a manner that allows the prevalence of one on others discussed in (Alexy, 2000)

[244] The first Law of Balancing, also known as the Substantive Law, states that "[t]he greater the degree of non-satisfaction of, or detriment to, one right or principle, the greater must be the importance

also used in the context of legal argumentation (Feteris et al., 2017, Ch. 7.5). The twofold internal and external relevance of Alexy's Laws of Balancing seem appropriate for dealing with conflicting scenarios.

5.2 The P-SAFETY model

The model presented hereafter consists of five principles - Security, Accountability, Fairness, Explainability, TransparencY (SAFETY) - enriched by one meta-principle - Privacy - that enables all the SAFETY-based recommendations to respect the datafication process of food behaviour related to individuals and groups. The following subsections illustrate and discuss each principle in detail. However, their constant interactions (highlighted by the multiple cross-references in the text) suggest that the Roadmap is not a mere "sum" of stand-alone principles, but should be read holistically.

5.2.1 Security

Security encompasses several dimensions, all related to issues regarding external threats to informations systems (Vedder, 2019). Threats can occur from the interaction of unauthorised third parties with the information system at stake (HLEG, 2019, p.17).

In the domain of interest, security pertains to a wide range of areas, including the technical protection of data warehouses, confidential private data, food consumption and background information (data security). At the same time, it also regards the technical robustness of AI systems and their capability to avoid fallacies, to be implemented in light of the *by-design* approach (AI security).

As regards data security, information sharing is desirable for the cross-validation of scientific data and often necessary for legal compliance. If, as argued, information exchange is also based on trust, a legitimate expectation of security is likely to arise among the involved entities. For these purposes, the functional role of security in ensuring trust noted by one institutional charter (BMWi, 2018, p.8) has to be remarked.

of satisfying the other" (substantive importance of reasons). The second Law of Balancing, also known as the "Epistemic Law", states that: "The more heavily an interference with a constitutional right weighs, the greater must be the certainty of its underlying premises"

In food safety risk assessment, data security follows the well-know dimensions of confidentiality, integrity and availability (CIA model) of the datasets (Olivier, 2002). Clarifications are thus needed to see how these dimensions can be integrated within the Roadmap.

Confidentiality is necessary to limit the access to private and personal (food consumption and background) information. Remarkably, the rationales underlying the confidentiality of these data are different: while the protection of commercially-sensitive information fosters the legitimate interests of private parties, the secrecy of personal data is necessary for reasons linked to fundamental rights to privacy and data protection. Security measures should be grounded on the conceptualisation of food consumption data as proxies for sensitive information. Unlawful processing activities may occur for illicit behaviours on legitimately processed data, e.g. beyond the purpose limitation principle. Individual food consumption data and background information might be used to predict the health status of individuals or for marketing purposes, hence the necessity of protecting this information from unlawful exploitation and data breaches.

As regards integrity, security should also be intended as the conceptual basis for safeguard measures that ensure that analysed data have not been altered. As remarked, data "poisoning" seriously threatens the validity of scientific findings and the credibility of all the stakeholders involved in food safety[245]. This dimension becomes relevant when we consider what has been remarked by AGID (AGID, 2018, p.30) when discussing the relationship between the security of machine learning systems and the construction of training datasets, according to the well-known mechanism 'garbage-in, garbage-out'[246].

Finally, with regards to availability, security measures should not hinder data sharing among national food safety authorities, risk assessors and risk managers. When safeguards are necessary to ensure confidentiality, their design should allow legitimate uses of data for the validation of assessment results consistently with the new provisions of the Transparency Regulation, copyright and data protection law.

Discussing AI security *strictu sensu*, it can be observed that, in light of the lower

[245] This was already observed when discussing the Monsanto Paper scandal in §2.4.2

[246] In general, it has been observed that poor quality training data generate erroneous (e.g. biased, fallacious, or simply wrong) outputs. To understand the relevance of guaranteeing the integrity of data used in the training phases of AI development, the MIT carried out the ”Norman” experiment (http://norman-ai.mit.edu). The Institute trained a conversational bot with different input data holding the same algorithm. Following training phases, the bot developed some sort of bipolarism: on the one hand, it displayed a regular interaction; on the other hand, it turned into a sociopath. Holding the training algorithm constant, the divergent aptitude of Norman reflects the quality of its training data

degree of autonomy of machine learning systems in our domain in comparison to others (e.g. self-driving cars or robots), the relevance of technical robustness is quite limited. However, the dimension of error handling (European Commission, 2020) shall not be overlooked, in particular when designing (BMWi, 2018, p.37) systems used to support human decisions with large-scale effects.

5.2.2 Accountability

The principle of Accountability can be found in all the aforementioned ethical Charters. The German document (BMWi, 2018, p.16) suggests that accountability frameworks are needed to generate trust towards machine learning systems, or our second-order trust. The Dutch document (SIGAI, 2019) takes an holistic approach to encompass three stages of AI development discussed hereafter.

In the design stage, accountability pairs with the replicability of the system's operations (HLEG, 2019, p.17). Ensuring this property is desirable in our domain since the validation of submitted or original studies cannot disregard the chance of experiment being replicated. When the studies rely on machine learning softwares, data and algorithms constitute part of the experimental setting and should favour its replicability to their maximum extent. This entails, *inter alia*, the necessity of identifying key elements of the mathematical model, the data labelling process, and other elements described under the "Explainability" principle.

In the monitoring stage, accountability implies the capability of verifying and audit the resources used in the course of risk assessment. This stage seems quite critical since EFSA's competences and financial resources might not suffice to ensure the monitoring of algorithms used by third parties when submitting scientific evidence or by the Authority itself. Case studies presented in Chapter 2 and summarised in Table 6.1 show that the scrutiny operated by EFSA can be performed with the support of machine learning systems, e.g. automatic literature reviews. Such techniques might also be performed over results generated with other machine learning approaches. Monitoring of algorithms seems then needed at every level of the scrutiny to prevent "cascade" accountability gaps.

Finally, in the redress stage, accountability is crucial to allocate liability for damage (Villani et al., 2018, p.113) or moral responsibility for the use of machine learning systems (SIGAI, 2019, p.5). However, redress represents a legal and governance challenge. Elsewhere we noted (§3.4.3) that EFSA's scientific output are not subject to the jurisdiction of the CJEU due to their non-bindingness, Moreover, the remit of EFSA non-contractual liability is limited and never tested before a Court. Then, we found particularly problematic the hypothetical in which EFSA receives results based on a functioning (i.e. nonfaulty) machine learning algorithm that suffers from the probabilistic error typical of stochastic approaches.

A possible solutions relies on the consideration that the Commission is the entity entitled to issue binding decisions - informed by EFSA's scientific opinions - for which it holds accountability. When adopting decisions, the Commission has to rely on the precautionary principle discussed above. Therefore, the principle can serve as a benchmark to allocate liability in the hypothetical: if probabilistic results cannot be guarantee a sufficient degree of certainty (e.g. a large range of plausible values in regression problems or a high number of false positives even in the case of high precision scores for classification algorithms), the precautionary principle is triggered. It follows that the most cautious measure (e.g. a temporary ban of a given product) is taken pending confirmatory results, perhaps with conventional methodologies. If this sort of mechanism is implemented, redress mechanisms for the use of machine learning techniques are reconciled with the consolidated redress scheme.

Mutatis mutandis, Accountability principle also governs the processing of personal data. On the one hand, this is true when individual food consumption data and background information are collected and stored since data controllers have to comply with data protection law (Pagallo et al., 2019); on the other hand, even though the GDPR and Regulation 2018/1725 are not directly applicable to aggregated data, the close relationship between the information type at stake and personal (individual and group) identity and the consequences of the processing activities for certain groups entail the necessity of taking into account the context in which such processing occurs, even beyond the scope of data protection law (Vedder and Naudts, 2017).

5.2.3 Fairness

In Chapter 2, the collection and the aggregation of food consumption data and background information data has been described as one of the key components of risk assessment. Then, Chapter 3 has revised the legal regime applicable to such information and identified risks linked to the processing of this information and its combination with non-personal data to identify the correct level of risk. From these premises, fairness is a crucial principle intended to minimise the effects of possible discriminations, in particular of individuals belonging to groups that can be drawn on the basis of food preferences.

In the AI Charters under scrutiny, Fairness can be intended from a *procedural* (or design) and a *substantive* perspective. From a *procedural* point of view, it has been described as the technical prevention of biases in results generated through machine learning techniques (Villani et al., 2018, p. 121). Discriminatory outcomes can result from the poor quality of the datasets, their incompleteness or imbalances (European Commission, 2020). This can be avoided by adopting technical measures (SIGAI, 2019, p.11). In its procedural dimension, fairness is also connected to accountability measures and redress mechanisms (HLEG, 2019, p.7).

From a *substantive* viewpoint, the use of machine learning techniques should be steered towards the minimisation of the negative consequences of existing discriminations and the accessibility of the benefits due to AI (Jobin et al., 2019). Substantive fairness also entails the prevention of new forms of wrongful differentiations (Vedder and Naudts, 2017).

According to Council Directive 2000/43/EC[247], discriminations can be direct or indirect[248]. However, only few elements, namely racial or ethnic origin can trigger the applicability of anti-discrimination legislation, hence its inadequacy to confront with other forms of discriminations, including the ones that originate on different, yet sensitive, grounds (Durante, 2019, p.252). In particular, data-driven forms of discrimination are particularly problematic due to the three reasons highlighted by Hacker (Hacker, 2018), i.e. their falling outside of the material scope of anti-discrimination law, the proliferation of indirect discrimination, and the placement of the burden to prove the discriminatory nature of the algorithm placed on discriminated individuals[249].

From the technical and legal analysis carried out in the previous Chapters, it emerges that individual discrimination is unlikely to occur. Data aggregation prevents the attribution of consumption patterns to specific individuals[250]. From a legal stand-

[247] Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin [2000] OJ-L 180/22

[248] Article 2 of the states that:

(a) direct discrimination shall be taken to occur where one person is treated less favourably than another is, has been or would be treated in a comparable situation on grounds of racial or ethnic origin;

(b) indirect discrimination shall be taken to occur where an apparently neutral provision, criterion or practice would put persons of a racial or ethnic origin at a particular disadvantage compared with other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are appropriate and necessary.

[249] As regards this last point, our considerations on data-driven fallacies §2.4.3 and the functioning of probabilistic modelling are of particular interest. Since discriminatory results can originate from functioning algorithms (i.e. algorithms that correctly execute all the planned instructions), assessing their unfair outputs might become even harder despite the availability of the source code and the training datasets

[250] Here, the assumption is that personal data *strictu sensu* are not accessed by unauthorised parties and eventually used in compliance with the applicable data protection law. It has to be remarked, however, that food consumption data collection occurs at individual level and access/distribution

point, EFSA scientific opinions do not produce legal effects on individuals and mostly affect groups[251].

In our domain, Fairness can then be discussed under both perspectives, which are inextricably linked. From a procedural standpoint, fairness can be understood as equal representativeness of food patterns. The datafication of food preferences and the use of dietary information for risk assessment purposes entails the risk that certain food patterns are under- or over- represented, thus triggering data-driven fallacies (§2.4.3). Such fallacies might generate discriminatory results, in particular when imbalanced datasets are used as training sets for machine learning algorithms. Beside unfair differentiation based on "regular" data, such as geographical provenance or gender, discrimination can also occur on the basis of personal information which reflect individual traits subsumed under the category of sensitive data when food preferences are associated e.g. to ethnic or religious groups.

From a substantive perspective, the correspondence between food preferences and personal identity has been noted in §2.4.1. In the light of the above considerations, risk assessment shall not increase existing discriminations and shall trait all food patterns equally. Despite the lack of studies suggesting any perpetration of this form of discrimination, an explicit committent of public and private entities to anti-discrimination measures is still missing despite the risks highlighted by the abundance of papers and documents on this topic, including institutional AI Charters. This is particularly relevant since non-traditional forms of discrimination - such as the ones based on vegetarianism or veganism - are yet unknown to anti-discrimination measures while being discussed in courts[252].

Fairness can ultimately serve as the rationale for technical and organisational measures intended to prevent discrimination based on dietary patterns. Such measures can ensure that due consideration is given to non-traditional or minoritarian food preferences when they are recorded and used for further analysis (*procedural* perspective), according to the trend identified as Big Data disparate impact (Barocas and Selbst, 2016). Such conceptualisation of *fairness-as-representativeness* is also grounded on the concept of statistical parity, i.e. the property that the demographics of those receiving positive (or negative) classifications are identical to the demographics of the population as a whole (Dwork et al., 2012)[253], regardless of ma-

rules discussed in Chapter 2 are enriched by contractual agreements, whose contents are unknown to the public. This prevents any further scrutiny on data misuses that can harm specific individuals

[251] A similar scenario is discussed in (Hallinan and de Hert, 2017) with regards to conclusions based on genetic information. Authors note that "The Regulation [...] was drafted on the presumption that the individual, and individual rights, were the primary target of protection."

[252] Case *Casamitjana v The League Against Cruel Sports* [2020] UKET 3331129/2018. A British Employment Tribunal found out that veganism is a protected characteristic under the UK Equality Act of 2010 for being a philosophical belief. See also §2.4.1

[253] As the technical domain of food safety has been constructed both on classification and regres-

chine learning deployment. The reference to Rawls (Rawls, 2009) in (Dwork et al., 2012) makes explicit that the notion of fairness presented by the authors is individual rather than collective (Sabelli and Tallacchini, 2017), hence the necessity of evaluating also its group-oriented dimension. Different solutions (namely, prejudicial remover techniques) have been proposed (Kamishima et al., 2012) and framed also in light of the Explainability principle discussed below (Zarsky, 2016). The most appropriate notion of fairness seems to be a group-based conceptualisation that promotes equality among food patterns that aggregate individual preferences reflecting identified clusters (vegetarians, vegans, ethnic minorities).

On the other hand, these measure support the effort to prevent forms of discrimination based on data reflecting personal identity when data protection law is not applicable due to data aggregation (*substantive* perspective). Moreover, if we consider the ongoing trends related to the use of *near* big data sources (e.g. mobile app-assisted self-recorded food consumption), the principle of Fairness can be linked to its conceptualisation under data protection law (discussed below) as a legal benchmark to verify that individual expectations of privacy are respected.

5.2.4 Explainability

Explainability is an ethical principle primarily intended to promote algorithmic transparency and prevent opaqueness and "black boxes". It has been endorsed by the Commission as a key technical requirement (European Commission, 2020) functional to the evaluation of fairness (European Commission, 2018). The German approach (BMWi, 2018, p.16) has identified its proximity to trust, as explainable machine learning models allows the assessment of legal compliance (Doshi-Velez, Kortz, et al., 2017; Mittelstadt, C. Russell, et al., 2019). The corollary of Explicability has been proposed by AI4People group (AI4People, 2018) and the HLEG (HLEG, 2019), which has referred to this principle as the capability of AI systems to communicate their operations and provide for a rationale for their output.

Consistently with our legal analysis, the domain of Explainability should be deemed different from the scope of Transparency *strictu sensu*. While the former concerns the ability to scrutinise the logic and the rationale underlying algorithmic results, the latter has been eventually conceptualised as a general attitude towards data disclosures for reasons of democratic oversight (§3.4.3). To avoid misconceptions and

sion problems, further clarifications are needed. Despite the occurrence of regression problems in the domain at stake, statistical parity affects the binary *at-risk/not-at-risk* classification of aggregated food consumption patterns, regardless of how the problem has been framed (e.g. in the case of logistic regressions) to promote consistency with food law terminology, it would be preferable to treat these principle separately.

As regards the principle of Explainability, the domain at stake provides food for thought. An EFSA-funded study ((IZSTO et al., 2017), reported in Table 6.3) shows awareness towards the issue of algorithmic opaqueness and displays scores regarding the capability to assess the logic underlying their results. Two intertwined sets of claims can thus follow. On the one hand, that it is necessary to strike balance between the degree of efficiency of machine learning techniques and the explainability of their results; on the other hand, that the precautionary principle can serve indirectly as a benchmark similarly to what has been discussed under the principle of Accountability.

Let us start from the first claim. Risk assessment concerns the discovery of unknown possible risks through scientific analysis. If the machine learning models deployed in this context are not auditable and their results are not explainable, it follows that EFSA will confront with a *ignotum per ignotius* situation, i.e. the scenario in which an explanation is more cumbersome than the phenomenon that the one it should clarify. This is not convenient in light of its goal of reducing uncertainty towards food-related risks, that is the ultimate objective of risk assessment[254].

As regards the second claim, we already noted that the precautionary principle does not apply to risk assessment activities and only pertains to the area of risk management. EFSA scientific outputs *informs* risk managers (Fig. 1.1), which in turn take decisions on the basis of the precautionary principle. Risk managers can allow for less cautious decisions only if the layers of uncertainty surrounding certain risks are erased to a threshold that is higher than the one needed to pass the precautionary test. When unexplainable machine learning models prevent a deep scrutiny of possible risks, the precautionary principle still applies. In other words, the opacity of machine learning models is an integral part of the scientific uncertainty that might lead to the "most cautious decision" to be taken by risk managers in accordance with the precautionary principle. Therefore, explainability and precaution are linked. Their relationship can be constructed as follows: the "most cautious decision" has to be taken every time the level of uncertainty due to the use of opaque machine learning algorithms is intolerably high according to a precautionary evaluation. When this is the case, a comparable conventional method should be preferred to verify the existence of risks. This indirect relationship also ensures a sufficient degree of consistency between Explainability and the existing legal framework, in

[254] From a broader perspective, the consideration of EFSA as an "autonomous epistemic agent" (Lynch, 2016) can reinforce the necessity of implementing explainable algorithms to increase its active participation to the epistemic aspects of risk assessment. In this perspective, explainable algorithms allow for the transformation of statistical correlations into epistemic conclusions by EFSA and remark its autonomy

particular as regards the accountability for the decisions that are made[255].

This is, of course, a hard trade-off. Viable alternatives may consist of researching how machine learning models deployed in this context can be made more explainable, consistengly with the approach to explainable AI (XAI) research promoted by the French charter (Villani et al., 2018).

The HLEG noted that the explanation "should be timely and adapted to the expertise of the stakeholder concerned. In addition, explanations of the degree to which an AI system influences and shapes the organisational decision-making process, design choices of the system, and the rationale for deploying it, should be available" (HLEG, 2019, p.18)[256]. It is thus possible to conceive the essential traits of explanations. In general, explanations can be given *ex-ante* and *ex-post* and should be comprehensive of several elements identified by Palmirani (Palmirani, 2020) when discussing explanations in automated decision-making (ADM) in the context of the GDPR. Explainable ADM targeted to individuals and explainability in our domain differ significantly due to the existence of specific norms granting a right to explanation (yet, debated among scholars (Doshi-Velez, Kortz, et al., 2017; Pagallo, 2020; Wachter, Mittelstadt, and Floridi, 2017)). However, the discussion on *what* would make algorithms explainable significantly affects our domain.

To prevent opaqueness of machine learning models applied to food safety risk assessment, essential elements[257] should be provided[258]. *Inter alia*, it is possible to lower the level of opaqueness by providing:

- *Ex-ante* elements:

    1. What mathematical models have been applied;

    2. How training, test and validation sets have been constructed (e.g. sources, missing data strategy, data cleaning strategy, measures to prevent biases, under- and over- fitting);

[255] (Tallacchini, 2014) has discussed the relationship between the precautionary principle and accountability in decision-making processes related to innovation in nano-technologies

[256] Doshi-Valez and Kim (Doshi-Velez and Kim, 2017) distinguish between *global* and *local* explanations. While global explanations refer to the general framework in which an automated decision has been taken (e.g. to detect biases), local explanaibility concerns the ability of giving reasons about a specific decision

[257] The list below has been drafted considering conclusions from Palmirani (Palmirani, 2020) who split the *ex-ante* from the *ex-post* explainability elements, then adapted to the technical findings emerged in Chapter II and EFSA cases studies displayed in Table 4 and Table 5. The list is also context-dependent, as some elements might be missing in practical scenarios

[258] These criteria should apply both in industry-to-EFSA, EFSA-to-Commission and EFSA-to-public information sharing depending on the entity that makes use of machine learning algorithms

3. How selection and grouping of individual food consumption data has occurred;

4. If the individuals entitled to label data dispose of sufficient expertise to fulfil their tasks, in the case of supervised learning algorithms.

- *Ex-post* elements:

  1. An explanation of its outputs understandable for their receiver (Explicability, see below)

  2. A comparison between the results obtained with the support of machine learning techniques and conventional methods

  3. Overall performance scores (accuracy, recall, F1, etc.)

  4. Detailed performance scores (accuracy, recall, F1, etc.) for food patterns

Against these findings, it might be argued that providing these elements is an excessive burden for commercial applicants or the Authority. While this argument might seem, *prima facie*, acceptable, it is worth considering the centrality of trust in the scenario at stake. The submission and subsequent publication of these elements is ultimately aimed to reinforce trust and to prevent that machine learning models put an additional layer of opacity and, thus, aversion towards the entities involved, including undertakings. On the one hand, the time span between these submissions and the renewal is sufficient to ensure return of investment both in financial and intangible assets (e.g. brand or institutional reputation); on the other hand, the submission of these elements is not revolutionary, as an effort is already made to submit and publish other information that results from considerable investments.

Explicability is a related ethical principle (Jobin et al., 2019) first proposed by the AI4People initiative (AI4People, 2018)[259] that expresses the practice to select an appropriate Level of Abstraction that fulfils the desired explanatory purpose, appropriate to the system and receivers of the explanation, deploy suitable persuasive arguments and finally provides explanations to the receiver of its outputs on the goals pursues when developing and deploys the AI system (Cowls et al., 2019). Explicability becomes necessary every time AI outputs need to be understood and interpreted by their receiver. Its remit is not limited to the industry-to-EFSA data sharing, but also embraces the EFSA-to-Commission relationships and, crucially, the EFSA-to-citizen scenario, i.e risk communication.

[259] AI4People group investigated two nuances of Explicability, namely "intelligibility" and "accountability", both of which have been kept into account in this Chapter

Explanations shall not nudge the explainee to refrain from critically questioning or contesting the decision (Mittelstadt, C. Russell, et al., 2019). The instrumentality of explanations to the right to contest individual ADM has been been noted by some authors (Palmirani, 2020; Wachter, Mittelstadt, and C. Russell, 2017). In the domain under scrutiny, the right to contest the decision is not applicable. However, a conceptual substitute is EFSA's institutional duty to critically evaluate scientific evidence coming from commercial applicants. Instead, when the Authority relies on machine learning systems (e.g. automated literature review) Explainability is functional to the transparency and the accountability of risk assessors (§3.4.1). Therefore, Explainability significantly correlates with EFSA's mandate in both cases.

5.2.5 Transparency

Thanks to the amendments brought by the Transparency Regulation, the EU food safety risk assessment legal framework has improved the capability of independent reviewers and authorities to carry out their activities by making more data available to them. At the same time, if the premises of the reform will be respected, all the stakeholders will eventually benefit from the gain in reputation and trust among citizens.

In the AI Charters, Transparency has multiple facets. First, it encloses what has been previously defined as Explainability (SIGAI, 2019, p.13) when it empowers individuals to scrutinise the logic and the criteria underlying certain decision-making processes that make use of Big Data and machine learning (BMWi, 2018, p.38). While this dimension has already been covered and unnecessary repetitions might generate confusion, it is necessary to underline that Explainability and Transparency dimensions are both means to allow the intelligibility of the algorithmic results. What might differ, especially in the context under discussion, is their goal. While Explainability is mainly aimed to minimise the opaqueness of certain machine learning algorithms to increase the epistemic soundness of their outcomes, food law Transparency revolves around other obstacles that prevent the foreseeability of health-related risks (e.g. IPRs) or layers of opaqueness in the activities of the Authorities.

The notion of transparency has been defined holistically to comprise data, algorithms and business models (HLEG, 2019, p.18) as a necessary prerequisite of auditability (Villani et al., 2018, p.15). Importance has been given to the relationship between algorithmic transparency and the accountability of public bodies when they make use of AI systems (AGID, 2018, p.11).

We noted that existing laws are more data-centric than algorithm-oriented. They seldom require the submission of programming codes used to perform analysis. A proactive and future-proof approach to Transparency might suggest to implement measures such as broadening the list of information to be disclosed by commercial applicants to include programming codes, input data and trained models to allow the replication of the experiment, or creating lists of algorithms and mathematical models that the industry has adopted when drafting submitted studies.

While the ways - "hard law", self-regulation, etc. - in which new transparency measures could be implemented will be left to future research consistently with the scope of the Roadmap, it is worth verifying their theoretical adequacy to the legal framework in place. When discussing the legal justifications of transparency, it has been noted that it consists of allowing citizens to foresee health-related concerns ("transparency-as-foreseeability") (§3.3.3) when environmental information is at stake and ensuring independence and accountability of the Authority (§3.4.1).

It has to be remarked that the shift towards an algorithm-oriented model necessarily implies some constraints to the measures intended to protect the investments in R&D made by the industry, hence they should be limited to what is necessary and proportionate to their overall goal, which is worth examining[260].

In both cases, a shift towards algorithms could be justified under the objectives of the existing regulatory framework. With regards to the independence and the accountability of the Authority, the release of details about the functioning of the algorithms deployed either by the industry or by the Authority itself is necessary to ensure that a) EFSA is kept "in the loop" and its outputs do not entirely depend on algorithms, and b) accountability gaps are prevented due to the absence of human oversight. When environmental information is at stake, the "transparency-as-foreseeability" criterion implies that details about algorithms are made available to the public to verify the correctness of their functioning and the findings related to human health that are generated with the support of these algorithms.

5.2.6 The question of Privacy: from SAFETY to P-SAFETY

Finally, let us discuss the relationship between SAFETY principles and privacy. Since we identified a human informational component of food safety risk assessment and discussed its ownership implications, this subsection aims to cast light on

[260] Instead of the "fostering trust" rationale, which is an original interpretation of this work, a safer starting point can be the recostruction of the CJEU case law discussed above. This is also to avoid the *petitio principii* or circular reasoning fallacy. This Roadmap is intended to foster trust in all the entities involved in food safety risk assessment. Therefore, the "fostering trust" rationale underlying transparency measures cannot be used as their sole justification in this context, despite its validity in the construction of the ownership model discussed before

what kind of privacy shall be discussed and how it relates to the SAFETY principles as a whole and with respect to each of them.

Both institutional and non-institutional AI Charters show unanimous consensus on privacy, hence the necessity of keeping it into account according to our methodology. It is conceived as the protection of the private sphere (AGID, 2018), both at individual and group level (Villani et al., 2018). When considered in its constitutional dimension in Germany, its role as a fundamental right is remarked (BMWi, 2018). With specific regard to machine learning techniques, due attention is given to the generation of training datasets that do not reflect biases or generate inaccuracies (European Commission, 2020).

As previously stated, AI Charters are purposively broad and embrace all the possible meanings of *privacy* in the sense given by Floridi (Floridi, 2013a, Ch.12.2), i.e. intrusion in physical, mental, decisional, and informational level[261]. However, in light of our technical contextualisation, it is first necessary to verify the what facets of privacy can be applied in our domain.

Mental and decisional privacy are not threatened by the use of machine learning techniques in food safety risk assessment due to the lack of any direct intervention on individuals' mind or decisions. This includes individuals who are surveyed in food consumption data collection stages. While it is true that EFSA outputs can have some degree of influence over consumers, they do not primarily aim to nudge or manipulate individuals and their effects in orienting preferences seem quite limited without the support of risk communication. Moreover, the discussion on whether such manipulation is likely to occur falls under the scope of risk communication rather than risk assessment. The physical intrusion in the private sphere seems quite limited as well, especially in comparison to other technologies covered by institutional documents (e.g. facial recognition or AI-supported IoT devices). Quite different would have been the case had real-time food consumption data collection systems been the state-of-the art. Lastly, while informational privacy and data protection might have a strong relevance in data processing activities, technical and legal evidence discourages its explicit endorsement. On the one hand, food patterns are usually aggregated or otherwise anonymised, thus limiting the scope

[261] Floridi argues in favour of a quaripartition of the concept of privacy: *physical* privacy protects the individual from tangible interferences against her or his body; *mental* privacy prevents others to manipulate one's mind and protects the psychological dimension of an individual; *decisional* privacy protects individuals from interferences in decision-making processes; *informational* privacy aims to protect individuals from interferences that related to facts that shall be not be disclosed. The concept of informational privacy is broader than data protection, as it does not only cover "information related to an identified or identifiable individual" but also "facts", which might be placed outside the scope of data protection law. In reality, however, this difference tends to disappear and this is particular true in the context at stake. As argued, the human behaviour of eating ("facts") is recorded and associated to a given individual ("data")

of data protection laws over processed data and the intrusion in individuals' private spheres; on the other hand, derogations of data protection laws for statistical and research purposes[262] consistently limit the remit of rights granted to protect 'raw' personal information (Palmirani, 2020).

For these reasons, an outright adoption of Privacy as a standalone principle would be wrong and likely to raise methodological concerns. Therefore, the SAFETY model could adopt informational privacy as a metaprinciple, i.e. a principle primarily intended to serve and integrate the SAFETY model. Such *meta-* formalisation of informational privacy does not entail that less importance should be given to it in comparison to other principles. Instead, this conceptualisation simply clarifies that privacy is included in the model "in relation to" (P-) to other principles rather than as an independent component. When informational privacy is conceptualised as data protection (Lynskey, 2014), the legal framework also embed "principles, general rights, concrete subjective rights and rules" (De Hert, 2017), whose interplay with the Roadmap shall be taken into account. In the light of the limited applicability of data protection laws in the framework under scrutiny, the principle-level discussion. Once clarified the relational nature of the Privacy principle, let us now discuss how this relationship unfolds with respect to each component of the SAFETY model.

The connection between Privacy and Security has already been introduced when discussing the implications of data processing activities with regards to individuals' food consumption and background information. We noted that, as these data might be used as proxies for sensitive inferences, data breaches and unlawful exploitations pose a serious threat to informational privacy. Alongside such consequentialistic reasons, an ontological approach to privacy (Floridi, 2005) might suggests that violations to these data constitute a breach of one's personal identity. Such approach seems appropriate in light of the nature of the personal (food consumption) data at stake, hence the need of prioritising data protection measures for the personal information stored and analysed in this context. The same holds true for "AI security", i.e. the minimisation of threats posed to individuals by AI systems. In light of the limited degree of autonomy of machine learning systems in the domain at

[262] Recital 156 of the GDPR states that: 'Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes'. In a similar fashion, Article 25(3) of Regulation 1725/2018 states that "[W]here personal data are processed for scientific or historical research purposes or statistical purposes, Union law, which may include internal rules adopted by Union institutions and bodies in matters relating to their operation, may provide for derogations from the rights referred to in Articles 17, 18, 20 and 23 subject to the conditions and safeguards referred to in Article 13 in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes"

stake, Privacy relates with this facet of Security when considering that the use of machine learning techniques might generated inferences that re-identify individuals and possibly their sensitive traits.

Privacy can be a guidance to evaluate Accountability for the individual, collective and social implications of personal data processing. This can be done by two sets of measures: on the one hand, privacy-oriented accountability *strictu sensu* requires that efforts to comply with data protection law are made[263] and demonstrated[264]. They include technical and organisational measures (data protection by design), staff training and records of the data protection activities (ICO, 2018). On the other hand, *latu sensu* accountability requires a risk-based aptitude towards the collective and social effects of large-scale data processing. While such formalisation of accountability may exceed the scope of data protection law, risks such as the possible re-identification or de-anonymization of surveyed individuals or data-driven biases towards certain groups identified by their 'datafied' food behaviours call data controllers to take responsibility for their data processing activities.

Likewise, the conceptualisation of Fairness could benefit from the Privacy-oriented consideration that food consumption data analysis can discriminate on grounds that consist of sensitive attributes of individuals. As we noted as regards Fairness, however, anti-discrimination law does not necessarily apply to all the grounds of discrimination that use food consumption data as proxies, hence the necessity of extending anti-discrimination measures beyond the material scope of anti-discrimination law. Hacker (Hacker, 2018) argues that data protection law and anti-discrimination provisions can be integrated when personal data are used to make decisions to tackle discrimination issues. This might have implications regarding *indirect* discrimination - the only possible in the context at stake - and group-level privacy (Floridi, 2017). At individual level, when conceptualised as a data protection principle[265], Fairness requires that personal data is processed in a way that does not harm data subjects. With the remit of ADM being limited in food safety risk assessment, Fairness and Privacy work jointly to ensure that adverse effects on individuals are minimised. This might trigger measures that prevent the unlawful exploitation of their data for purposes other than risk assessment, limited access to data, and, from a broader perspective, that other data protection law principles are respected [266]. With

[263] Article 5(2) of the GDPR and Article 4 of Regulation 2018/1725 state that "[T]he controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 [the other data protection principles, *ed*]" See also (De Hert, 2017). In the context of data transmission, Art. 9(1) of Regulation 2018/1725 is also relevant.

[264] Instead, we noted elsewhere (§3.1.3) that the protection given to personal data at the collection stage is highly jeopardised

[265] Article 5(1) of the GDPR; Article 4(1) Regulation 2018/1725

[266] Authors (Sabelli and Tallacchini, 2017) have underlined that such conceptualisation of "fairness" in data protection might be insufficient to ensure a fair data processing due to the *ex-ante* adoption of machine learning algorithms and the existence of *ex-post* remedies only in data protec-

regard to two of them - data minimisation[267] and accuracy[268] - trade-offs are necessary. On the one hand, data minimisation requires that the least possible amount of data is collected, hence the need of validating the information obtained from the data subject (listed in Table 6.4) in light of data collection needs; on the other hand, in light of the limited remit of data subjects' rights, data accuracy requires an effort to be made to adapt recorded food consumption data to individual preferences over time. These two elements bridge the gap with machine learning techniques, which require a large quantity of up-to-date data to produce accurate results.

A large and growing number of scholars is debating on the relationship between data protection law and Explainability, especially in light of the provisions enshrined in Article 22 of the GDPR (Palmirani, 2020; Wachter, Mittelstadt, and Floridi, 2017, *inter alia*). We noted that the remit of data protection law is restricted due to the statistical and research purposes of the processing for risk assessment and no ADM is made in the course of risk assessment. Regarding profiling[269], it might be the case that certain data processing activities fall within the remit of predictions related to data subject's health when exposed to pathogens. The nature of data processing made by EFSA does not seem to cover this possibility. However, when considering industry-led studies that process dietary intake data with the support of predictive algorithms, the fate of inferred information might be relatively unknown to the data subject[270]. It is then necessary to clarify the extent to which individual predictions may occur and their effects on risk assessment activities. This is particularly true when considering the existence of "data conglomerates" such as the Bayer-Monsanto company which might use additional information to generate predictions on the basis of food consumption data. When this is the case, data subjects should be given *ex-ante* and *ex-post* intelligible details about the data processing.

The relationship between Privacy and Transparency might be cumbersome to grasp. Transparency is a key principle of data protection law[271] as it contributes to the in-

tion law. Therefore, they called for a synergic inclusion of data protection law and collective values, including trust

[267] Article 5(1)(c) of the GDPR; Article 4(1)(c) of Regulation 2018/1725

[268] Article 5(1)(d) of the GDPR; Article 4(1)(d) of Regulation 2018/1725

[269] "Profiling" consists of 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 analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements" (Article 4(1)(4) of the GDPR, Article 3(1)(5) of Regulation 2018/1725). For an exhaustive review of GDPR's provisions with regards to profiling activities, including concrete cases, please refer to the work done by Gonzales and De Hert (González and de Hert, 2019)

[270] While this is undoubtedly out of the scope of the EU food legislation, this consideration might be of interest for entities (including non-profit) and scholars that investigate the implications of personal data processing and its interplay with specific domain, e.g. the processing within the context of pharmaceuticals

[271] Article 5(1) of the GDPR; Article 4(1) Regulation 2018/1725

formational self-determination of the data subject by making her or him aware of the nature of the processing, the entities involved and so on, ultimately fostering her or his free choice. However, the meaning attributed to Transparency in the Roadmap - in essence, the widest possible availability of data and contextual information to replicate studies - differ from the one conferred in the context of data protection law. Therefore, when linked to the Roadmap, Privacy shall act a constraint to Transparency in giving access to raw personal information to third parties. This is necessary to prevent unlawful exploitations of data, including the breaches of purpose limitation principle[272]

5.3 Possible implementations of the Roadmap

Findings from the Roadmap might be of interest for theoretical contributions in the field of AI ethics. However, it is also possible to discuss their practical implications by theorising certain implementations that could translate the Roadmap into practice.

The Roadmap could affect all the entities involved in the domain of interest. Since risk assessors, the industry, and consumers (including those selected for food consumption surveys) are linked by a trust-based relationship also for their data-related interactions, it follows that any implementation of the Roadmap will have effects - even disparately - on all the entities involved and on the trustworthiness of the whole system.

A "naïve" legal translation would be unlikely, at least in the short term. Considering the highly controversial nature of data-related provisions and the complexity of the norms in force, EU-level reforms of the domain at stake might take time despite the pace of technological advancements calling for new regulation. The Transparency Regulation has come into existence 17 years after the first version of the GFLR and no further amendments are expected anytime soon. Instead, the Commission could adopt some of the provisions of the Roadmap (e.g. additional data requirements discussed under "Explainability") as implementation acts, similarly to other interventions presented in Chapter 3. While this might ensure a sufficient degree of bindingness, it might further complicate the regulations in force. Likewise, the CJEU could rely on some of interpretations provided by the Roadmap (e.g. on the algorithm-inclusive remit of "environmental information") in the course of its activity.

EFSA could adopt some provisions as technical recommendations. While EFSA

[272] Article 4(1)(b) of the GDPR; Article 4(1)(b) of Regulation 2018/1725

regulatory powers are limited by its competences, the Authority might rely on its technical influence to techno-regulate certain phenomena, in particular those linked to the deployment of machine learning techniques by the industry. At the same time, EFSA's scientific bodies could adopt the principles of our Roadmap as their own guidelines. In both cases, the level of bindingness will be lower than the one of "hard law", but likely sufficient to ensure a certain degree of validity, as other initiatives (e.g. data standardisation) prove.

Food business operators could implement the Roadmap as a form of self-regulation. This possibility brings along all the concerns regarding "ethics washing" identified in the previous Chapter, hence the necessity of coordinating the effort of undertakings with the supervisory powers of the Authority. The relationship with Good Laboratory Practices[273] is also to be defined.

The Roadmap could serve ad an additional evaluation guideline for the latest (to date) EU initiative regarding AI Trustworthiness, i.e. the ALTAI (The Assessment List on Trustworthy Artificial Intelligence)[274]. This tool, released by the HLEG in July 2020, is intended to provide a self-evaluation instrument for organisations willing of assessing the trustworthiness of their AI tools by verifying their adequacy to the seven key requirements - Human Agency and Oversight; Technical Robustness and Safety; Privacy and Data Governance; Transparency; Diversity, Non-discrimination and Fairness; Societal and Environmental Well-being; Accountability - identified by the EU Commission and discussed above. It has been noted that some of these requirements are particularly significant in the domain at stake. Therefore, the Roadmap could help organisations in identifying, integrating or aligning their practices to the general requirements identified by the Commission. Vice versa, the Roadmap could be used by the Commission to highlight areas of particular risks from the domain at stake (e.g. the conclusions and the replicability of studies relying on machine-learning) and act accordingly.

Further implementations which exceed the narrow scope of this thesis can be theorised. For instance, one could consider the "altruistic purposes" in data sharing highlighted by the proposed "Data Governance Act"[275]. Considering the current (February 2021) state of discussion, one possible implementation of the Roadmap

[273] Good laboratory practice (GLP) is a standardised way of planning, performing and reporting laboratory-based studies to ensure a high standard of quality and reliability. It encompasses several requirements, which involve the use of gloves, face masks, and selected hardware. As regards data, they shall be kept secured by providing a "chain of custody". In the EU, GPL is mandatory in chemicals, food additives, novel Foods and their ingredients, and plant protection products

[274] https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment

[275] European Commission Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) COM/2020/767 final

is the one proposed by the draft Regulation. Following the proposal, one or more competent bodies, designated by the Member States, "which collect and process data made available for altruistic purposes" can register and support physical or legal persons, including public administration bodies, to *donate* their data[276]. Data *donation* is conceptualised as a re-use, i.e. an use intended for purposes other than the initial one for which the data were produced[277]. Such re-use does not create an obligation to release data subject to confidentiality rules and shall be done according to rules concerning commercial confidentiality, statistical confidentiality[278], the protection of intellectual property rights of third parties[279], protection of personal data[280]. Public sector bodies may also impose an obligation to re-use only pre-processed data, and pre-processing shall to anonymize/pseudonymise personal data or delete commercially confidential information, including trade secrets[281].

The proposed framework requires further research activities that I will briefly introduce in §6.3. However, it can be preliminary observed that the possible adoption of this Regulation can somewhat interact with the P-SAFETY model presented in this thesis. Our conclusive framework could be translated at Member State level especially as regards the careful balance of between interests such as data security & confidentiality, transparency, and privacy. As always, it is worth reminding that the proposed model is a "local" implementation of high-level principles. From the preliminary commentary provided above, however, our framework seems consistent with the drafted Regulation especially in the key role attributed to data for the purposes of public administrations. Data sharing for altruistic purposes can also be read in the light of the trust-oriented approach of our P-SAFETY model when contextualised in food safety. For instance, the presented model could be further enhanced by the voluntary sharing of commercially sensitive data by undertakings with the goal of increasing trust, especially in those areas where the disclosure can be still mandated by Courts. Data users could also be registered NGOs which could perform independent reviews. This is, however, a far-reaching goal that necessarily requires several steps - including the adoption of the Data Governance Act - for its full implementation.

[276] Art. 7(2)(c) of the Proposed Data Governance Act

[277] Art. 2(2) of the Proposed Data Governance Act

[278] With regards to confidentiality, a specific provision (Art. 5(8) of the Proposed Data Governance Act) obliges public bodies to not disclose confidential information

[279] See also Art. 5(7) of the Proposed Data Governance Act. In particular, public bodies cannot rely on the Database Directive's *sui generis* protection to to prevent the re-use of data or to restrict re-use

[280] Art. 3(3) of the Proposed Data Governance Act

[281] Art. 5(3) of the Proposed Data Governance Act

5.4 Chapter Synopsis

This Chapter has presented the final outcome of this dissertation, i.e. an ethical Roadmap intended to support and integrate the existing legislation concerning agri-food risk assessment data-related provisions. This content has been presented as the transposition of high-level principles identified in Chapter 4 within the legal and technical context of food safety risk assessment, according to the approach widely discussed in other parts of this dissertation.

The Roadmap has been modelled by taking into account the necessity of fostering trust between citizens, risk assessors and AI/machine learning softwares (Fig. 5.1). The model consists of five core SAFETY principles - Security, Accountability, Fairness, Explainability, Transparency - and one metaprinciple - Privacy - whose relational nature consists of its integration within the SAFETY model as an corollary, prerequisite or constraint.

On the one hand, Security concerns the integrity of confidential and personal data, in particular those intended to train machine learning systems or used to draw inferences when used as scientific evidence. On the other hand, Security-as-error-handling for machine learning systems with large-scale effects has been considered relevant and discussed.

Accountability has been framed, on the basis of background literature and AI charters, in three dimensions - design, monitoring, and redress - that, taken together, shall guarantee that the machine learning systems are a) programmed consistently with the need of replicating scientific studies, b) audited to monitor their behaviour, and c) deployed in a manner that ensure damage repair. At the same time, Accountability has been identified as a key component of compliance with the applicable data protection law.

The principle of Fairness has been conceptualised under a *procedural* - i.e. proportionate representativeness of food patterns used as source of evidence - and a *substantive* perspective - i.e. non-discrimination among groups that share certain food habits or similar traits recorded by food consumption data.

General considerations on Explainability have been linked to the peculiarities of the domain at stake. This entails, as a rule of thumb, that non-explainable outputs of machine learning softwares shall trigger the precautionary principle, thus leading to the taking of the "most cautious decision" by food safety risk managers. To prevent the application of the precautional principle, *ex-ante* and *ex-post* essential elements shall be submitted alongside raw data. A list of key features has been drafted by taking into account contributions on Explainability of machine learning systems.

Transparency comprises data and algorithms. Despite the efforts made by lawmakers in the Transparency Regulations as regards the public availability of data, a niche regarding the availability of algorithms has been identified. The Roadmap has proposed to include algorithms and operational data used or generated by industrial studies among the notion of environmental information, in accordance with the interpretation ("transparency-as-foreseeability") provided by the CJEU in its recent case law.

Informational Privacy has been identified as a meta-principle for being *in relation to* other principles rather than as a standalone component. With regards to Security, Privacy should be then considered as a justification to adopt technical measures to protect these data from external threats. Privacy can be a guidance to evaluate Accountability for the collective and social implications of personal data processing even beyond the scope of data protection law. The conceptualisation of Fairness could benefit from the Privacy-oriented consideration that food consumption data analysis can discriminate on grounds that consist of sensitive attributes of individuals; Privacy makes Explainability crucial to protect the fate of personal information analysed via machine-learning techniques by giving *ex-ante* and *ex-post* intelligible details about the data processing, in particular for industry-led studies. Lastly, Privacy is a necessary constraint of Transparency needed to protect individuals from unlawful access and exploitation of their data.

Furthermore, the Chapter has identified some possible implications of the Roadmap. They range from the "hard law" model to a "good practice" implementation, with several degrees of bendiness. In particular, one viable way of implementing the Roadmap could be its *local* integration with the ALTAI proposed by the EU HLEG.

6

Final remarks and future research

6.1 Thesis Synopsis

In this investigation, the aim was to find appropriate answers to one research question and three sub-questions. They originated from the necessity of discussing the positive and negative implications of an ongoing trend of "datafication" that the food safety risk assessment system is experiencing. The chosen methodology was to identify three research areas - broadly intended as "technology", "law", and "ethics" - that taken together could provide an holistic perspective of the research issue and contribute to find appropriate solutions. Their integration has been realised by combining high-level ethical Charters and the technical and legal domain identified in the first steps of the research. Let us now turn to give, in summary, answers to the questions posed in the Introduction.

The following 1-page synopses mirror the research question and sub-questions discussed in the Introduction, with a short restatement of the research methodology. They are also simplified, with some sacrifice in precision made in the hope of easier understanding by a broader audience.

1st Research Sub-Question

QUESTION. How are data transmission and analysis reshaping the ownership and the governance of data in the agri-food safety domain?

METHODOLOGY. A literature review has been carried out to understand technical advancements in Big Data collection and sharing practices, alongside the discovery of state-of-the art data analysis techniques. Its outputs have been presented according to a classification (Big data sources *vis-à-vis* data analysis techniques). Then, these results have been discussed holistically as informational components to bridge the gap with other sections.

ANSWER. Food safety's ongoing "datafication" process is a trend according to which data (*rectius*, Big data) consist of the main source of analysis of food-related hazards. The importance of data is growing in all the sector of food safety risk analysis, in particular in risk assessment. On the one hand, a trend in collecting and standardising large quantities of data can be observed. This information tends to be frequently updated by the many sources that indirectly contribute to the EFSA Data Warehouse (agri-food businesses, EU Member States, and so on) by submitting their data. On the other hand, to maximise the potential of data in supporting risk assessment activities, machine learning is the set of tools to which EFSA and the food industry have devoted attention in recent years.

In particular, it seems that EFSA is making a "probabilistic turn": alongside traditional (deterministic) methodologies, new paradigms involving the use of probabilistic modelling are emerging. Areas such as the automatic review of the literature, exposure assessment, and outbreaks monitoring, are some of the most affected domains.

The growing relevance of Big data and the deployment of machine learning techniques entail the necessity of balancing the investments made by the industry in research and development with the scrutinisability of industrial and, in turn, EFSA's findings by the public. This can be done by acknowledging the presence of three informational components - the human, the natural, and the machine-generated one - within the same ecosystem. When looking at the inferences made possible thanks to Big data and, possibly, machine learning techniques, new paradigms of ownership and governance emerge.

2^{nd} Research Sub-Question

QUESTION. How can we balance the need of property rights emerging from agri-food industry, the calls for more transparency coming from public society and rights over personal data?

METHODOLOGY. A legal research was performed to reply to this research question. The underlying methodology was the one of "legal formants" by Sacco (Sacco, 1991), which operates at a level of abstraction capable of identifying hidden peculiarities of the legal systems at stake. To restrict the area of investigation, the EU legal system has been selected as the core topic, with occasional reference to EU Member States. Following this approach, EU food safety legislation, rulings of the CJEU and reviewed academic commentaries were selected as primer background materials.

ANSWER. The balance between these clashing interests can be done by first re-considering the traditional, monolithic approach to data ownership (i.e. one entity being entitled to own the data exclusively) and accepting the premises of a model of distributed ownership. Its peculiarity is that EFSA, the industry, citizens and individuals whose food consumption data is collected enjoy a *quasi*-ownership of data. In this perspective, EFSA is responsible for the dynamic allocation of access and distribution rights. Openness and transparency measures are guided by the necessity of preserving trust in the Authority and among all the entities involved. This intuition is supported by a) the novelty of the Transparency Regulation, which restates the overriding public interest in the disclosure of environmental information and mandates EFSA to act proactively to disseminate data submitted by commercial applicants to a wider extent than before; b) the amendments brought by the Transparency Regulation to EU sectoral legislation to align it with the general presumption of public interest; c) conclusions reached by the CJEU when discussing the concept of "environmental information" and identifying the rationale underlying disclosure measures in the foreseeability of health effects on individuals; d) academic commentaries that progressively discuss a new paradigm of ownership.
Case law and academic literature have shown some degree of inconsistency in identifying the rationales underlying transparency and openness measures, the former being justified by the need of a democratic risk assessment, the latter by the necessity of ensuring collaborative forms of risk assessment. Neither of these approaches is satisfying: on the one hand, since risk assessment does not amount to a decision-making process, there is no necessity of supporting democracy in a scientific discussion. On the other hand, the amount of individuals capable of actively contributing to the risk assessment is low.
The proposed approach, which consists of the necessary prerequisite of the distributed ownership model discussed above, is that trust among stakeholders is the essential elements that justifies information sharing measures.

3rd Research Sub-Question

QUESTION. What rules, principles and values should be reflected into the data governance models and frameworks that regulate the behaviour of the entities involved in EU agri-food safety risk assessment?

METHODOLOGY. Consistently with the territorial scope of the investigation, EU and EU Member States (Germany, France, the Netherlands, Italy) ethical charters on AI were selected and critically evaluated in light of AI ethics contributions coming from the literature. Other non-institutional charters represent auxiliary source of analysis.

ANSWER. Principles enshrined in institutional AI Charters represent a viable way to integrate and align technical and legal provisions that regulate the behaviour of the entities involved in food safety risk assessment. Several justifications are presented in support of this conclusion. First, the attempts made by these Charters, consistently with the academic literature on this point, highlight the centrality of trust as an essential element for a safe deployment of machine learning techniques across all the domains in which AI might have an impact. The legal attempt made by the Transparency Regulation domain is to prioritise trustworthiness of the risk assessment, hence the continuity of trust-oriented approaches. Second, provisions enshrined in institutional AI Charters are not intended to replace the existing (or forthcoming) legislation but to verify its resilience to the challenges posed by AI/machine learning. This is convenient in our domain because the 2019 reform made significant progresses in data-related matters and no further reforms seem plausible in the short period. Third, there is a significant degree of consensus among these principles, verified by trusted reviewers and commentators, which can be then used to find appropriate data governance solutions for the domain of agri-food safety risk assessment. However, some adaptations are necessary to prevent certain methodological fallacies - including ethics shopping - while contextualising high-level AI charters to the technical and legal specifications of EU food safety risk assessment.

Research Question

QUESTION. How can data ownership and data governance be shaped to maximise the benefits and minimise the risks of using and processing Big Data in the context of EU Agri-Food safety risk assessment?

METHODOLOGY. Ethical principles can be used to align the existing framework to the advancement of Big data analysis and machine learning. With these three components - ethical, legal and technical frameworks - already been identified, candidate principles can be selected and verified in light of pre-defined criteria consistent with the domain at stake. This is necessary to avoid misconceptions in what is technically feasible or legally required or admitted, to prevent "ethics shopping" and, eventually, to make research results robust.

ANSWER. The answer is provided in form of a Roadmap, a short and concise document that can be used to interpret and align the existing data ownership and data governance frameworks to the challenges posed by Big Data collection, storage and analysis, including by means of machine learning. The model has been presented as a non-hierarchical and non-exclusive list of principles that, taken together, can help EFSA and the industry involved to increase their trustworthiness by managing their data according to certain *desiderata*. The presented model consists of five core principles - Security, Accountability, Fairness, Explainability, TransparencY (SAFETY) - and one metaprinciple - Privacy (P-) - that can be implemented to adapt the technical and legal domain of food safety risk assessment to the ongoing datafication trend in a manner that risks are prevented and benefits are maximised.
Possible implementations - simply introduced consistently with the scope of this thesis - range from "hard law" to monitored self-regulation, including the possible alignment with the ALTAI (the Assessment List on Trustworthy Artificial Intelligence) which represent the most recent (to date) product of the EU Commission HLEG on AI.

6.2 Significance of this study

This work contributes to the existing knowledge of several domains, consistently with the many research areas investigated.

This study consists of an in-depth look into an often under-estimated - yet, highly debated - field of study (i.e. food safety), with regard to one of its most controversial sub-domains (i.e. data used for risk assessment purposes). Hence, this contribution also aims to foster the debate surrounding a research area to which the scientific literature on Big Data, ownership, and governance has not devoted adequate attention, especially in comparison to "neighbour" subject matters such as healthcare and pharmaceutical[282].

Agri-food safety could then become of prime importance. It consists of a unique ecosystem in which several data-types - non-personal, personal, mixed, observed, derived, inferred, and so on - co-exist. Such concurrence raises questions regarding the level of access to these data, the protection of intellectual property, the public relevance of such information, and so forth. This contribution also casts light on some of these issues, with the hope that other contributors will accept the challenges raised by this domain.

Among these information-types, food consumption data present unique challenges widely discussed in this study. Not only revolve they around the scope of data protection law, but also their use in aggregated forms might raise concerns that go beyond the remit of the GDPR and Regulation 2018/1725. In both cases, this work contributes to these lines of research with an applied case study highlighting the need to synergise the debates on data protection law and other data-related concerns, including group privacy and discrimination.

The relative novelty of discussing Big Data and machine learning emerging issues in an applied domain also brings along methodological innovations. This has been done only by bringing the level of maturity in the AI & ethics discussion to the "next level", i.e. the translation of high-level principles into practical domains. It might be argued that this process might be stopped in case of legal intervention by lawmakers, especially in the case of "heavy hand" legislation. While acknowledging that explicit provisions regulating AI might prevent the adoption of the principle-based approach, it might be useful to restate that trustworthiness does not necessarily conjugate with legal compliance. To put it differently, legal compliance and the adoption *ad abuntantiam* of a principle-based aptitude that aims to correlate high-level

[282] The link is provided by certain similarities that can be found especially in the legal regime. Pharmaceutical, likewise regulated products, need approval at EU level following a scientific evaluation. Processed data include sensitive (health) data of individuals subject to trials (Savonitto, 2019)

principles to applied domains can work together to ensure that trust is maintained among all the entities involved. This also consistent with the "soft ethics" approach that the Roadmap intend to follow.

With regards to trustworthiness, this study also strengthens the centrality of trust. While aforementioned studies have identified the *intrinsic* necessity of Trust in human-machine relationships, the scenario discussed in this research also presents an *external* need of a fiduciary liaison that is independent from the use of AI/machine learning techniques, i.e. what has been referred to as "First-order Trust". However, the presence of a human-machine trust-based relationship (our "Second-order Trust") reveals the existence of a new order ("Third-order Trust") which consists of the connection between citizens and the use of advanced data analytics techniques. While this is somewhat similar to the Second-order for being a human-to-machine relationship, Third-order Trust also shows the presence of an authoritative intermediary (EFSA).

The centrality of EFSA in this study has also to be remarked. While recognising its role as functional to the assessment-management division of competences with the EU Commission, it has been argued that, under the new Transparency Regulation, EFSA will become crucial in attributing access and distribution rights to all the entities involved, thus reinforcing its centrality among the EU risk analysis governance mechanisms. This study acknowledges the fundamental role played by EFSA in the current datafication scenario: while data assume a growing relevance, the Authority acts as an epistemic gatekeeper which finds answers and removes layers of uncertainty surrounding the effects of newly invented industrial products, novel foods, unprecedented pathological threats, and so on. From a strict data governance perspective, this finding is relatively new due to the novelty of the Transparency Regulation.

6.3 Limitations and future research

The questions raised by this studies are multifaceted and involve several research areas, including bioinformatics, ethics, law and governance. There are viable paths for further research that would be fruitful areas of investigation consistently with this research domain.

From a methodological perspective, the approach taken by this thesis is somewhat innovative: while combining high-level ethical principles and a legal and technical domains might resemble applied ethics to some extent, investigated ethical principles were already "applied" to the domain of AI. While consolidated methodologies have been selected, identified and adopted for each research area of this dissertation (technology, law, ethics), the extent to which the combination of the three of them performed in this study is a viable methodology for other studies remains to be elucidated.

The technical premises of this dissertation are based on the assumption - yet, supported by a concrete interest shown by EFSA, independent studies and commercial entities - that an ongoing datafication trend can be observed at every level of food safety risk assessment, from information gathering to data analysis and knowledge extraction. The level of innovation in this field is evolving constantly, with occasional sudden peaks such as the automation of literature reviews. Therefore, research in data ownership and governance has to keep pace with cutting edge technologies deployed in this sector.

With the Transparency Regulation still to enter into force, the commentary provided in Chapter 3 has to be revised in light of EFSA's implementations. Undoubtedly, contributions from scholars active in food and environmental law will provide further insights on the new Regulation and its effectiveness. Still on the legal side, the relationship of our findings and Corporate Social Responsibility is undoubtedly an area of valuable investigation purposively neglected by this dissertation, as well as the topic of Big Data & competition. Furthermore, with the food market becoming increasingly global and the progressive extenuation of the food chain, legal comparison is a research methodology that can become useful in evaluating how different jurisdictions deal with the risks posed by the ongoing datafication trend.

The relationship between the Proposed Data Governance Act and the P-SAFETY model can be conceptualised as a mutual support. On the one hand, the Regulation could inspire measures for Member States' food safety authorities for the re-use of some of the information-types discussed in this dissertation; on the other hand, our Roadmap and its conclusion will be likely challenged by the adoption of the Regulation, if passed. For instance, the notion of "data holder", i.e. any legal person or data subject who, in accordance with applicable Union or national law, has the right to grant access to or to share certain personal or non-personal data under its control[283], and "data user", i.e. any natural or legal person who has lawful access to certain personal or non-personal data and is authorised to use that data for commercial or non-commercial purposes[284] seem quite consistent with the distributed ownership model presented in §3.4.2 and can be used to describe the subjective positions covered by each entity from time to time. However, this research area still demands time and efforts, especially in the light of the provisional nature of the Proposed Regulation.

As regards Trust, the identification of other forms of Third-order Trust with au-

[283] Art. 2(5) of the Proposed Data Governance Act

[284] Art. 2(6) of the Proposed Data Governance Act

thoritative intermediaries could be a possible directions for future research. Other domains might be the ones linked to the use of AI/Machine Learning tools by law enforcement authorities, judges, public administrations and so on. Likewise, a comparison with neighbour legal domains (e.g. pharmaceuticals, chemicals) would be beneficial to evaluate similarities and differences among areas characterised by scientific uncertainty and the necessity of risk evaluations ultimately affecting Trust.

Considering the scope of an ethics-based Roadmap, in the wake of "data altruism" sharing of data to third countries might be another implementation of an ethics-based Roadmap. Not considering sharing with third countries is a known limitation of this thesis[285]. If we broaden its geographic scope, the P-SAFETY model can undoubtedly be enriched by considering that the EU can lead the transfer of pre-processed data to third countries to contribute to novel forms of risk assessment. This naturally requires major adaptations to the model.

Much of the findings of this dissertation, including its main output i.e. the Roadmap, are theoretical and have to be put into practice. When discussing possible implementations, some proposals have been made, yet in a purely hypothetical form. More work is then needed to assess how this introductory framework could be translated into practice. Such translation can occur both at legal and technical level, hence the need of further research in both fields of study. The cross-fertilisation of heterogeneous research areas seems unavoidable for any future work.

[285] I would like to acknowledge of the external reviewers who highlighted this limitation

Appendix

Table 6.1: EFSA's external report (IZSTO et al., 2017) - Machine Learning Techniques vs conventional methods

Area of interest	Goal	Input Data	Output	Algorithms
Exposure assessment	Assessing health risks associated to the consumption of red meat and/or processed meat	EPIC simulated dataset including processed meat consumption and personal characteristics including (age, sex, Hours of physical activity a week, haemoglobin, height, weight)	Health status after a 5-year period (classification problem "colorectal cancer" vs "non-cancer")	Naïve Bayes, Conditional Inference Trees, Recursive Partitioning and Regression Trees, k-Nearest Neighbour, Multi–Layer Perceptron (neural network), Multi–Layer Perceptron Ensemble (deep neural network), Support Vector Machine, Random Forest, bagging, boosting, Linear Discriminant Analysis, Logistic Regression, Quadratic Discriminant Analysis
Feed additive risk assessment	Estimating an appropriate Benchmark dose lower level based on the toxicological studies provided; compliance with Regulation (EC) No 1831/2003 on feed additives	Data recording the effects of different doses, provided by a company	A benchmark dose lower level based on the provided data, one for each algorithm	Conditional inference tree, Decision tree, K-Nearest Neighbour, multilayer perceptron with one hidden layer, multilayer perceptron ensemble, support vector machine, Random Forest, multivariate additive regression splines, Principal Component Regression, partial last squared regression, canonical powered partial last squares relevance vector machine
Monitoring of transmissible spongiform encephalopathies in sheep and goats	Assessing the impact of prevention and eradication measures in the EU	Time series from EU Member States monitoring programmes	A regression model that highlights and predict existing (until 2011) and future trends (2012)	Canonical powered partial least squares, conditional inference tree, K-Nearest Neighbor, Multi–Layer Perceptron (neural network), Multi–Layer Perceptron Ensemble (deep neural network), Naïve Bayes, Principal Component Regression, Partial Least Squares Regression, Random forest, Support Vector Machine
Daphnia Magna ecotoxicological studies	Identify concentration levels of certain toxicants that immobilise Daphnia Magna	Experimental data	Predictive toxicology model for untested samples	Conditional inference tree, decision tree, K-Nearest Neighbor, Multi–Layer Perceptron Ensemble (deep neural network ensemble), Support Vector Machine, Random Forest, Linear Discriminant Analysis, Logistic Regression.
Food Pyramid and portions	Developing suggestions for portions size according to nutrient intake controlling the amount of calories, fat, saturated fat, cholesterol, sugar or sodium in the diet.	MyPiramid dataset (US Department of Agriculture (USDA)): 1,000 commonly eaten foods and common portions	Degree of association in menu composition between vegetables and diary and meat products	Lasso regression method
Clinical research errors	Analysis of nephron function in response to micropunture	Experimental data on 75 rats	Regressions comparing different experimental methods (fewer rats, more observations VS more rats, less observations)	Linear Regression

Table 6.2: EFSA's external report (IZSTO et al., 2017) - Machine Learning Techniques applied to food safety risk assessment: case studies

Area of interest	**Goal**	**Input Data**	**Output**	**Algorithms**
Salmonella	Data quality assurance, i.e. to detect errors in current data submission in comparison to previously submitted data and to detect the record prevalence of a *salmonella* serovar	Datasets from the European Union Summary Reports on Zoonoses over the period 2011-2014 available on EFSA website	Computation of missclassification error rate (classification)	Random forest, Logistic Regression
Salmonella	Detection of latent pattern of epidemiological concern, i.e. find similarities in years/country	Datasets from the European Union Summary Reports on Zoonoses over the period 2011-2014 available on EFSA website	Visualisation of the estimated probability presence	Clustering, Partitioning Around Medoids
Foodborne outbreaks	Train a Superlearner to predict risk of hospitalization in food borne outbreak.	Food-Borne Outbreaks annual datasets (food-borne outbreaks, the number of human cases, deaths, number of hospitalized individuals) until 2011	Prediction model for hospitalisations in 2012	Superlearner (package in R) composed by Random Forest, Gradient Boosting Machine, Support Vector Machine, cross-validated
Antimicrobial resistance	Understanding the relationship between prevalence of zoonoses and antimicrobial resistance	Two aggregated datasets (a time-series and experimental data from laboratories)	A classification “resistant” or “not resistant” zoonosis; added probability of combinations of zoonoses and environmental variables	Random Forests (classification and regression)
Antimicrobial resistance	Predicting the lower resistant concentration	Two aggregated datasets (a time-series and experimental data from laboratories)	30 prediction	Support Vector Machine

Table 6.3: EFSA’s external report (IZSTO et al., 2017) - Machine Learning Techniques applied to food safety risk assessment: case studies

Algorithm Name	**Label**	**Problem**	**Computational Complexity**	**Transparency**
Clustering	Unsupervised	Clustering	Low	Poor
Conditional inference tree	Supervised	Classification	Medium	Good
Decision tree	Supervised	Classification	Medium	Good
K-Nearest Neighbor	Supervised	Classification	High	Good
Lasso	Supervised	Regression	-	-
Linear Discriminant Analysis	Unsupervised	Dimensionality Reduction	Low	Good
Linear Regression	Supervised	Regression	Low	Good
Logistic Regression	Supervised	Classification	Low	-
Multi–Layer Perceptron	Supervised	Classification	High	Poor
Multi–Layer Perceptron Ensemble	Ensemble	Classification	High	Poor
Multivariate adaptive regression splines	Unsupervised	Regression	-	-
Naïve Bayes	Supervised	Classification	Low	Good
Partial Least Squares Regression	Unsupervised	Dimensionality Reduction	-	-
Partitioning Around Medoids	Unsupervised	Clustering	Medium	Poor
Principal Component Regression	Unsupervised	Dimensionality Reduction	Low	Good
Quadratic Discriminant Analysis	Unsupervised	Dimensionality Reduction	Low	Good
Random Forest	Ensemble	Classification	High	Poor
Recursive Partitioning and Regression Trees	Supervised	Classification	Medium	Good
Superlearner	Ensemble	Regression	High	Poor
Support Vector Machine	Supervised	Classification	Medium	Poor

Table 6.4: EFSA structural metadata elements of personal data collection (EFSA, 2018b)

Name	Description	Optional	dataType	Catalogue	Data Protection
ACTIVITY	Description of the activity level	yes	text(250)		no
AGE	Age in years	no	number(6,2)		no
BIRTHDAY	Birth day	yes	number(2,0)		yes
BIRTHMONTH	Birth month	yes	number(2,0)		yes
BIRTHYEAR	Birth year	yes	number(4,0)		yes
COMMENTSSUBJECT	Text field to be used in order to provide additional information about the subject or to report on possible problems related to him/her	yes	text(250)		yes
COUNTRY	Country of the dietary survey	no	text(400)	COUNTRY	no
EDUCATIONF	Description of the current education level or highest diploma obtained by the father	yes	text(400)	EDUCATION	no
EDUCATIONM	Description of the current education level or highest diploma obtained by the mother	yes	text(400)	EDUCATION	no
EDUCATIONS	Description of the current education level or highest diploma obtained by the subject	yes	text(400)	EDUCATION	no
ENRGYINTAKE	Average energy intake over the survey period in Kcal per day	yes	number(20,10)		no
ETHNIC	Self-defined ethnic group	yes	text(250)		yes
FANTDAY	Date of the first anthropometric measurements (day)	yes	number(2,0)		yes
FANTMONTH	Date of the first anthropometric measurements (month)	yes	number(2,0)		no
FANTYEAR	Date of the first anthropometric measurements (year)	yes	number(4,0)		no
GENDER	Gender	no	text(400)	GENDER	no
GEO	Region, area or city of residence	yes	text(400)	NUTS	yes
HEIGHT	Height in cm from the first measurement	no	number(20,10)		no
LABOURF	Labour status of the father of the subject	yes	text(400)	LABOR	no
LABOURM	Labour status of the mother of the subject	yes	text(400)	LABOR	no
LABOURS	Labour status of the subject	yes	text(400)	LABOR	no
MHEIGHT	Method used to measure height	no	text(400)	MTYP	no
MWEIGHT	Method used to measure body weight	no	text(400)	MTYP	no
NHOUSEHOLD	Size of household-number of individuals in the household	yes	number(20,10)		no
ORSUBCODE	Unique subject identifier	no	text(50)		yes
PANSWER	Person who provided the answer	no	text(400)	PANSWER	no

PROFESSF	Professional category of the father of the subject	yes	text(400)	PROFESS	no
PROFESSM	Professional category of the mother of the subject	yes	text(400)	PROFESS	no
PROFESSS	Professional category of the subject	yes	text(400)	PROFESS	no
SANTDAY	Date of the second anthropometric measurements (day), if any	yes	number(2,0)		yes
SANTMONTH	Date of the second anthropometric measurements (month), if any	yes	number(2,0)		no
SANTYEAR	Date of the second anthropometric measurements (year), if any	yes	number(4,0)		no
SHEIGHT	Height in cm from the second measurement, if any	yes	number(20,10)		no
SPECDIET	Subject identified as having particular eating pattern	yes	text(400)	DIETTYPE	no
SPECIALCON	Subject identified as being in special conditions	no	text(400)	SCON	no
SURVEY	Acronym of the dietary survey	no	text(50)		no
SWEIGHT	Body weight in kg from the second measurement, if any	yes	number(20,10)		no
UNOVREP	Subject identified as under or over reporter	yes	text(400)	UOREP	no
WEIGHT	Body weight in kg from the first measurement	no	number(20,10)		no
WF	Weighting factor used to normalize for age groups, gender, regions Ö	yes	number(20,10)		no

Bibliography

References for Chapter 1: Introduction

Abrams, M. (2014). *The origins of personal data and its implications for governance*. URL: http://informationaccountability.org/wp-content/uploads/Data-Origins-Abrams.pdf (cit. on p. 16).

Ahmed, T. and I. de Jesús Butler (2006). "The European Union and human rights: An international law perspective". In: *European Journal of International Law* 17.4, pp. 771–801 (cit. on p. 3).

AI4People (2018). *AI4People | Atomium*. URL: https://www.eismd.eu/ai4people/ (cit. on pp. 37, 147, 186, 189).

Alemanno, A. (2014). "Unpacking the principle of openness in EU law: transparency, participation and democracy". In: *European Law Review* (cit. on pp. 7, 124, 126).

Alemanno, A. and S. Gabbi (2016). *Foundations of EU food law and policy: Ten years of the European food safety authority*. Routledge (cit. on pp. 2, 4, 42, 47, 61, 62, 79, 125, 131, 140, 141).

Ayala, A. and B. M. Meier (2017). "A human rights approach to the health implications of food and nutrition insecurity". In: *Public Health Reviews* 38.1, p. 10 (cit. on p. 3).

BBC (2018). "'All protection steps taken' after BSE diagnosis". In: *BBC News*. URL: https://www.bbc.com/news/uk-scotland-north-east-orkney-shetland-45954225 (cit. on p. 2).

Bevir, M. (2012). *Governance: A Very Short Introduction*. Very Short Introductions. OUP Oxford. URL: https://books.google.it/books?id=ozjcWIfho08C (cit. on p. 27).

Borgman, C. L. (2015). *Big Data, Little Data, No Data: Scholarship in the Networked World*. The MIT Press (cit. on p. 21).

British Academy and Royal Society (2017). *Data management and use: governance in the 21st century*. URL: https://royalsociety.org/-/media/policy/projects/data-governance/data-management-governance.pdf (cit. on p. 27).

— (2019). *data-ownership-rights-and-controls-October-2018.pdf*. URL: https://royalsociety.org/-/media/policy/projects/data-governance/

data-ownership-rights-and-controls-October-2018.pdf (cit. on p. 22).

Brown, P., R. G. Will, R. Bradley, D. M. Asher, and L. Detwiler (2001). “Bovine spongiform encephalopathy and variant Creutzfeldt-Jakob disease: background, evolution, and current concerns.” In: *Emerging infectious diseases* 7.1, p. 6 (cit. on p. 2).

Cai, X. Q., G. H. Liu, H. Q. Song, C. Y. Wu, F. C. Zou, H. K. Yan, Z. G. Yuan, R. Q. Lin, and X. Q. Zhu (2012). “Sequences and gene organization of the mitochondrial genomes of the liver flukes Opisthorchis viverrini and Clonorchis sinensis (Trematoda)”. In: *Parasitology research* 110.1, pp. 235–243 (cit. on p. 9).

Cappè, S., M. Gilsenan, E. O’Dea, J. Richardson, and D. Verloo (2019). “The future of data in EFSA”. In: *EFSA Journal* 17.1, e17011 (cit. on pp. 5, 42, 51, 65).

Clark, A. and D. Chalmers (1998). “The extended mind”. In: *analysis* 58.1, pp. 7–19 (cit. on p. 18).

Corea, F. (2019). “AI Knowledge Map: how to classify AI technologies”. In: *An Introduction to Data*. Springer, pp. 25–29 (cit. on pp. 18, 19).

De Mauro, A., M. Greco, and M. Grimaldi (2015). “What is big data? A consensual definition and a review of key research topics”. In: *AIP conference proceedings*. Vol. 1644. 1. AIP, pp. 97–104 (cit. on p. 13).

DECODE project (2020). *Common Knowledge: Citizen-led data governance for better cities*. URL: https://decodeproject.eu/publications/common-knowledge-citizen-led-data-governance-better-cities (cit. on pp. 22, 24, 135).

Dumbill, E. (2013). *Making sense of big data* (cit. on p. 14).

Durante, M. (2017). *Ethics, Law and the Politics of Information: A Guide to the Philosophy of Luciano Floridi*. The International Library of Ethics, Law and Technology. Springer Netherlands (cit. on p. 16).

Durante, M. (2019). *Potere computazionale: L’impatto delle ICT su diritto, società, sapere*. Mimesis (cit. on pp. 7, 125, 184).

EFSA (2011b). “Shiga toxin-producing E. coli (STEC) O104:H4 2011 outbreaks in Europe: Taking Stock”. In: *EFSA Journal* 9.10, p. 2390. URL: https://efsa.onlinelibrary.wiley.com/doi/abs/10.2903/j.efsa.2011.2390 (cit. on p. 2).

— (2014b). “The European Union Summary Report on Trends and Sources of Zoonoses, Zoonotic Agents and Food-borne Outbreaks in 2012”. In: *EFSA Journal* 12.2, p. 3547 (cit. on p. 2).

— (2015b). “Principles and process for dealing with data and evidence in scientific assessments”. In: *EFSA Journal* 13.6, p. 4121 (cit. on pp. 5, 10, 64, 65).

European Commission (2020). *Commission White Paper on Artificial Intelligence - A European approach to excellence and trust*. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. (Accessed on 05/22/2020) (cit. on pp. 18, 140, 148, 151, 182, 184, 186, 192).

Falagas, M. E., E. I. Pitsouni, G. A. Malietzis, and G. Pappas (2008). “Comparison of PubMed, Scopus, web of science, and Google scholar: strengths and weaknesses”. In: *The FASEB journal* 22.2, pp. 338–342 (cit. on p. 33).

FAO (1975). *The state of food and agriculture*. (Accessed on 07/09/2019). URL: http://www.fao.org/3/h3100e/h3100e.pdf (cit. on p. 3).

— (1983). *World Food Security: a Reappraisal of the Concepts and Approaches* (cit. on p. 2).

— (2018). *The State of Food Security and Nutrition in the World 2018*. URL: http://www.fao.org/3/i9553en/i9553en.pdf (cit. on p. 2).

FDA (2017). *BAM: Parasitic Animals in Foods*. URL: https://www.fda.gov/food/laboratory-methods-food-safety/bam-parasitic-animals-foods (cit. on p. 9).

Firican, G. (2018). *Data governance maturity models - IBM | LightsOnData*. URL: https://www.lightsondata.com/data-governance-maturity-models-ibm/ (cit. on p. 26).

Floridi, L. (2005). “The ontological interpretation of informational privacy”. In: *Ethics and Information Technology* 7.4, pp. 185–200 (cit. on pp. 23, 134, 193).

— (2006). “Information Ethics, Its Nature and Scope”. In: *SIGCAS Comput. Soc.* 36.3, pp. 21–36. URL: http://doi.acm.org/10.1145/1195716.1195719 (cit. on p. 36).

— (2008). “The method of levels of abstraction”. In: *Minds and machines* 18.3, pp. 303–329 (cit. on p. 36).

— (2013b). *The philosophy of information*. Oxford University Press (cit. on p. 15).

— (2014). *The fourth revolution: How the infosphere is reshaping human reality*. OUP Oxford (cit. on pp. 7, 72).

— (2018). “Soft Ethics and the Governance of the Digital”. In: *Philosophy and Technology* 31.1, pp. 1–8 (cit. on pp. 7, 149).

— (2019a). *The five principles key to any ethical framework for AI - NS Tech*. URL: https://tech.newstatesman.com/policy/ai-ethics-framework (cit. on p. 37).

Floridi, L., J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, et al. (2018). “AI4People—An ethical framework for a good AI society: opportunities, risks, principles, and recommendations”. In: *Minds and Machines* 28.4, pp. 689–707 (cit. on pp. 37, 162).

Floridi, L. and J. W. Sanders (2004). “On the morality of artificial agents”. In: *Minds and machines* 14.3, pp. 349–379 (cit. on p. 18).

Floridi, L. and M. Taddeo (2016). *What is data ethics?* (Cit. on pp. 31, 35, 36).

Fossa, F. (2017). “What is Moral Application? Towards a Philosophical Theory of Applied Ethics”. In: *Applied Ethics. The Past, Present and Future of Applied Ethics*. Ed. by C. for Applied Ethics and P. H. University, pp. 34–49 (cit. on p. 35).

Gartner (2008). *Gartner Introduces the EIM Maturity Model*. URL: https://pdfs.semanticscholar.org/ca3b/13f65a37d7b0a44287899710112e2c5afc4e.pdf (cit. on p. 26).

Gilsenan, M. (2015). “Data handling: Observatories-databases-data storage-legal framework EFSA data collection”. In: *Options Méditerranéennes. Series A: Mediterranean Seminars*. CIHEAM-IAMZ, Zaragoza (Spain)-EFSA, European Food Safety Authority, Parma (cit. on pp. 11, 43, 45, 50).

Global Open Data Index (2019). *What is Open Data according to the Open Definition?* URL: https://index.okfn.org/faq/ (cit. on p. 22).

Griffith, C. J. (2006). “Food safety: where from and where to?” In: *British Food Journal* 108.1, pp. 6–15 (cit. on p. 6).

Grimm-Samuel, V. (1991). “On the mushroom that deified the Emperor Claudius”. In: *The Classical Quarterly* 41.1, pp. 178–182 (cit. on p. 6).

Grindle, M. S. (2007). “Good enough governance revisited”. In: *Development policy review* 25.5, pp. 533–574 (cit. on p. 27).

Gruni, G. (2018). “The right to food and trade law in the external relations of the European Union with developing countries”. PhD thesis. University of Oxford (cit. on p. 3).

House Of Lords Select Committee (2018). “Ai in the uk: ready, willing and able”. In: *House of Lords* 36 (cit. on p. 21).

IBM (2014). *Infographic: The Four V’s of Big Data | IBM Big Data and Analytics Hub*. URL: https://www.ibmbigdatahub.com/infographic/four-vs-big-data (cit. on p. 14).

— (2016). *The 5 V’s of big data - Watson Health Perspectives*. URL: https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/ (cit. on p. 14).

ICO (2017). *Big data, artificial intelligence, machine learning and data protection*. URL: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (cit. on p. 16).

Jiménez, B., C. Maya, G. Velásquez, F. Torner, F. Arambula, J. A. Barrios, and M. Velasco (2016). “Identification and quantification of pathogenic helminth eggs using a digital image system”. In: *Experimental parasitology* 166, pp. 164–172 (cit. on p. 9).

Johnson, B. L. and M. Y. Lichtveld (2017). *Environmental Policy and Public Health*. CRC Press. URL: https://books.google.lu/books?id=fzg7DwAAQBAJ (cit. on p. 3).

Kaisler, S., F. Armour, J. A. Espinosa, and W. Money (2013). “Big data: Issues and challenges moving forward”. In: *2013 46th Hawaii International Conference on System Sciences*. IEEE, pp. 995–1004 (cit. on p. 14).

Kantardzic, M. (2011). *Data mining: concepts, models, methods, and algorithms*. John Wiley and Sons (cit. on pp. 18, 32).

Krapohl, S. (2004). “Credible commitment in non-independent regulatory agencies: A comparative analysis of the European agencies for pharmaceuticals and foodstuffs”. In: *European Law Journal* 10.5, pp. 518–538 (cit. on p. 4).

Kuner, C., L. Bygrave, C. Docksey, and L. Drechsler (2020). *The EU General Data Protection Regulation (GDPR): A Commentary*. Oxford University Press. URL: https://books.google.it/books?id=CBELtAEACAAJ (cit. on p. 16).

Ladley, J. (2012). *Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program*. The Morgan Kaufmann Series on Business Intelligence. Elsevier Science. URL: https://books.google.it/books?id=CpeAYWaTScYC (cit. on p. 26).

Laney, D. (2001). *3D Data Management: Controlling Data Volume, Velocity, and Variety*. Tech. rep. META Group. URL: http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (cit. on p. 14).

Logan, D. (2010). *What is Information Governance? And Why is it So Hard?* URL: https://blogs.gartner.com/debra%7B%5C_%7Dlogan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/ (cit. on p. 27).

Lombardi, O., F. Holik, and L. Vanni (2016). "What is Shannon information?" In: *Synthese* 193.7, pp. 1983–2012 (cit. on p. 15).

Mahmoud, S. (2019). "Sharing and caring". In: *IPPR Progressive Review* 26.1, pp. 78–89 (cit. on p. 22).

Martin, E. A. (2009). *A dictionary of law*. OUP Oxford (cit. on p. 21).

Marvin, H. J., E. M. Janssen, Y. Bouzembrak, P. J. Hendriksen, and M. Staats (2017). "Big data in food safety: An overview". In: *Critical Reviews in Food Science and Nutrition* 57.11, pp. 2286–2295 (cit. on pp. 7, 53).

Mayer-Schönberger, V. and K. Cukier (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt (cit. on p. 6).

McCarthy, J., M. L. Minsky, N. Rochester, and C. E. Shannon (2006). "A proposal for the Dartmouth summer research project on artificial intelligence, august 31, 1955". In: *AI magazine* 27.4, pp. 12–12 (cit. on p. 18).

McCrudden, C. (2008). "Human dignity and judicial interpretation of human rights". In: *european Journal of international Law* 19.4, pp. 655–724 (cit. on p. 3).

McNeely, C. L. and J.-o. Hahm (2014). "The big (data) bang: Policy, prospects, and challenges". In: *Review of Policy Research* 31.4, pp. 304–310 (cit. on p. 14).

Microsoft (2019). *Configure the user connections Server Configuration Option - SQL Server | Microsoft Docs*. URL: https://docs.microsoft.com/en-gb/sql/database-engine/configure-windows/configure-the-user-connections-server-configuration-option?view=sql-server-2017andviewFallbackFrom=sql-server-2017%7B%5C%%7D7D. (cit. on p. 22).

Mittelstadt, B. and L. Floridi (2016). "The ethics of big data: current and foreseeable issues in biomedical contexts". In: *Science and engineering ethics* 22.2, pp. 303–341 (cit. on p. 13).

Moor, J. H. (1985). "What is computer ethics?" In: *Metaphilosophy* 16.4, pp. 266–275 (cit. on p. 36).

Morley, J., C. C. Machado, C. Burr, J. Cowls, I. Joshi, M. Taddeo, and L. Floridi (2020). "The Ethics of AI in Health Care: a Mapping Review". In: *Social Science & Medicine*, p. 113172 (cit. on p. 7).

Müller, V. C. and N. Bostrom (2016). “Future progress in artificial intelligence: A survey of expert opinion”. In: *Fundamental issues of artificial intelligence*. Springer, pp. 555–572 (cit. on p. 18).

Nomenclature Committee of the International Society for Microbiology, S. S. et al. (1934). “The genus salmonella lignieres, 1900”. In: *The Journal of hygiene* 34.3, p. 333 (cit. on p. 6).

OECD (2019). *OECD Legal Instruments*. URL: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (cit. on p. 37).

Oracle (2013). *MDM Maturity Model*. URL: http://www.oracle.com/us/products/applications/master-data-management/mdm-maturity-model-1887940.pdf (cit. on p. 26).

Ostrom, E., R. Calvert, and T. Eggertsson (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Political Economy of Institutions and Decisions. Cambridge University Press. URL: https://books.google.it/books?id=4xg6oUobMz4C (cit. on pp. 22, 25).

Pagallo, U., P. Casanovas, and R. Madelin (2019). “The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data”. In: *The Theory and Practice of Legislation*, pp. 1–25 (cit. on pp. 27, 30, 147, 152, 167, 172, 183).

Pasquale, F. (2015). *The black box society*. Harvard University Press (cit. on pp. 10, 20).

Pattaro, E., H. Rottleuthner, R. A. Shiner, A. Peczenik, and G. Sartor (2005). *A treatise of legal philosophy and general jurisprudence*. Vol. 1. Springer (cit. on p. 34).

Peel, M. (1997). “Hunger strikes: Understanding the underlying physiology will help doctors provide proper advice”. In: *BMJ* (cit. on p. 1).

Piantadosi, C. (2003). *The Biology of Human Survival: Life and Death in Extreme Environments*. Oxford University Press, pp. 43, 52 (cit. on p. 1).

Psevdos, G., F. M. Ford, and S.-T. Hong (2018). “Screening US Vietnam veterans for liver fluke exposure 5 decades after the end of the war”. In: *Infectious diseases in clinical practice (Baltimore, Md.)* 26.4, p. 208 (cit. on p. 9).

Rodotà, S. (2015). *Il diritto di avere diritti*. Gius. Laterza and Figli Spa (cit. on p. 23).

Rusconi, G. (2016). “Food Safety and Policy in the European Union”. In: *International Food Law and Policy*. Springer, pp. 451–483 (cit. on pp. 11, 80, 81, 110).

Russell, S. and P. Norvig (2010). “Artificial intelligence: a modern approach”. In: (cit. on pp. 17, 18, 57, 154).

Sacco, R. (1991). “Legal formants: a dynamic approach to comparative law (Installment I of II)”. In: *The American Journal of Comparative Law* 39.1, pp. 1–34 (cit. on pp. 34, 203).

Sartor, G. (2016). *L’informatica giuridica e le tecnologie dell’informazione: Corso di informatica giuridica*. Vol. 2. G Giappichelli Editore (cit. on p. 31).

Seiner, R. S. (2014). *Non-Invasive Data Governance: The Path of Least Resistance and Greatest Success*. Technics Pub. URL: https://books.google.it/books?id=Xo3XBgAAQBAJ (cit. on p. 27).

Shannon, C. E. (1948). "A mathematical theory of communication". In: *Bell system technical journal* 27.3, pp. 379–423 (cit. on p. 14).

Simpson, C. (2016). "Data Protection under Food Law Post: in the Aftermath of the Novel Foods Regulation". In: *Eur. Food & Feed L. Rev.* 11, p. 309 (cit. on pp. 5, 100, 129, 130).

Soares, S. (2015). *Data governance tools: Evaluation criteria, Big Data governance, and alignment with enterprise data management*. Mc Press (cit. on p. 26).

Spedicato, G. (2016). "Digital lending and public access to knowledge". In: *Intellectual Property and Access to Im/material Goods*. Edward Elgar Publishing (cit. on p. 24).

Sripa, B., J. M. Bethony, P. Sithithaworn, S. Kaewkes, E. Mairiang, A. Loukas, J. Mulvenna, T. Laha, P. J. Hotez, and P. J. Brindley (2011). "Opisthorchiasis and Opisthorchis-associated cholangiocarcinoma in Thailand and Laos". In: *Acta tropica* 120, S158–S168 (cit. on p. 9).

Stewart, W. K. and L. W. Fleming (1973). "Features of a successful therapeutic fast of 382 days' duration". In: *Postgraduate medical journal* 49.569, pp. 203–209 (cit. on p. 1).

Szajkowska, A. (2012). *Regulating food law: risk analysis and the precautionary principle as general principles of EU food law*. 7. Wageningen Academic Pub (cit. on p. 4).

Tamò-Larrieux, A. (2018). "Mapping the Privacy Rationales". In: *Designing for Privacy and its Legal Framework*. Springer, pp. 27–43 (cit. on pp. 23, 134).

The Data Governance Institute (2015). *Definitions of Data Governance - The Data Governance Institute*. URL: http://www.datagovernance.com/adg%7B%5C_%7Ddata%7B%5C_%7Dgovernance%7B%5C_%7Ddefinition/ (cit. on p. 27).

The Data Warehousing Institute (2013). *Transforming Data with Intelligence*. URL: https://tdwi.org/pages/maturity-model/big-data-maturity-model-assessment-tool.aspx?m=1 (cit. on p. 26).

United Nations Committee Economic, Social and Cultural Rights (1999). *International Covenant on Economic, Social and Cultural Rights*. URL: https://undocs.org/E/C.12/1999/5 (cit. on p. 3).

Wende, K. (2007). "A model for data governance-Organising accountabilities for data quality management". In: *ACIS 2007 Proceedings*, p. 80 (cit. on p. 26).

Wong, K.-W., K.-M. Lam, and W.-C. Siu (2001). "An efficient algorithm for human face detection and facial feature extraction under different conditions". In: *Pattern Recognition* 34.10, pp. 1993–2004 (cit. on p. 20).

Ziegler, J., C. Golay, C. Mahon, and S. Way (2011). *The fight for the right to food: lessons learned*. Springer (cit. on p. 3).

References for Chapter 2: Data analysis practices in the context of EU food safety risk assessment

Abbar, S., Y. Mejova, and I. Weber (2015). “You tweet what you eat: Studying food consumption through twitter”. In: *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, pp. 3197–3206 (cit. on p. 53).

AGES, C. Vlachou, and D. Hofstädter (2019). “Joint venture on the further development of chemical exposure assessment by use of probabilistic modelling”. In: *EFSA Journal* 17, e170905 (cit. on p. 57).

Alemanno, A. and S. Gabbi (2016). *Foundations of EU food law and policy: Ten years of the European food safety authority*. Routledge (cit. on pp. 2, 4, 42, 47, 61, 62, 79, 125, 131, 140, 141).

Ambrus, Á., Z. Horváth, Z. Farkas, E. Dorogházi, J. Cseh, S. Petrova, P. Dimitrov, V. Duleva, L. Rangelova, E. Chikova-Iscener, M.-L. vaskainen, H. Pakkala, G. Heinemeyer, O. Lindtner, A. Schweter, A. Trichopoulou, A. Naska, W. Sekuła, S. Guiomar, C. Lopes, and D. Torres (2013). “Pilot study in the view of a Pan-European dietary survey – adolescents, adults and elderly”. In: *EFSA Supporting Publications* 10.11, 508E. URL: https://efsa.onlinelibrary.wiley.com/doi/abs/10.2903/sp.efsa.2013.EN-508 (cit. on p. 46).

Archer, E., G. Pavela, and C. J. Lavie (2015). “The inadmissibility of what we eat in America and NHANES dietary data in nutrition and obesity research and the scientific formulation of national dietary guidelines”. In: *Mayo Clinic Proceedings*. Vol. 90. 7. Elsevier, pp. 911–926 (cit. on p. 52).

Article 29 Working Party, A. (2015). *Letter to Paul Timmers’ Annex on health data in apps and devices*. URL: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf (cit. on p. 61).

Astill, J., R. A. Dara, M. Campbell, J. M. Farber, E. D. Fraser, S. Sharif, and R. Y. Yada (2019). “Transparency in food supply chains: A review of enabling technology solutions”. In: *Trends in Food Science and Technology* (cit. on p. 51).

Batis, C., M. A. Mendez, P. Gordon-Larsen, D. Sotres-Alvarez, L. Adair, and B. Popkin (2016). “Using both principal component analysis and reduced rank regression to study dietary patterns and diabetes in Chinese adults”. In: *Public health nutrition* 19.2, pp. 195–203 (cit. on p. 59).

Bisgin, H., T. Bera, H. Ding, H. G. Semey, L. Wu, Z. Liu, A. E. Barnes, D. A. Langley, M. Pava-Ripoll, H. J. Vyas, et al. (2018). “Comparing SVM and ANN based machine learning methods for species identification of food contaminating beetles”. In: *Scientific reports* 8.1, pp. 1–12 (cit. on p. 59).

Bouzembrak, Y., M. Klüche, A. Gavai, and H. J. Marvin (2019). “Internet of Things in food safety: Literature review and a bibliometric analysis”. In: *Trends in Food Science and Technology* (cit. on p. 51).

Bouzembrak, Y. and H. J. Marvin (2019). “Impact of drivers of change, including climatic factors, on the occurrence of chemical food safety hazards in fruits and vegetables: A Bayesian Network approach”. In: *Food Control* 97, pp. 67–76 (cit. on p. 41).

Brillat-Savarin, J. A. (1841). *Physiologie du goût*. Charpentier (cit. on p. 61).

Bryson, J. J. and P. P. Kime (2011). “Just an artifact: Why machines are perceived as moral agents”. In: *Twenty-Second International Joint Conference on Artificial Intelligence* (cit. on p. 74).

Cappè, S., M. Gilsenan, E. O’Dea, J. Richardson, and D. Verloo (2019). “The future of data in EFSA”. In: *EFSA Journal* 17.1, e17011 (cit. on pp. 5, 42, 51, 65).

Castañón, C. A., J. S. Fraga, S. Fernandez, A. Gruber, and L. d. F. Costa (2007). “Biological shape characterization for automatic image recognition and diagnosis of protozoan parasites of the genus Eimeria”. In: *Pattern Recognition* 40.7, pp. 1899–1910 (cit. on p. 59).

Cherno, M. (1963). “Feuerbach’s" Man is what He Eats": A Rectification”. In: *Journal of the History of Ideas*, pp. 397–406 (cit. on p. 61).

Cherry, E. (2006). “Veganism as a cultural movement: A relational approach”. In: *Social Movement Studies* 5.2, pp. 155–170 (cit. on p. 62).

EFSA (2011a). “Activities, Processes and Quality Assurance Elements on Data Collection Programmes with Member States”. In: *EFSA Supporting Publications* 8.3, 127E (cit. on pp. 43, 45, 47).

— (2014a). “Guidance on the EU Menu methodology”. In: *EFSA Journal* 12.12, p. 3944 (cit. on pp. 46, 96).

— (2015a). “Conclusion on the peer review of the pesticide risk assessment of the active substance glyphosate”. In: *EFSA Journal* 13, p. 4302 (cit. on p. 64).

— (2015b). “Principles and process for dealing with data and evidence in scientific assessments”. In: *EFSA Journal* 13.6, p. 4121 (cit. on pp. 5, 10, 64, 65).

— (2015c). *Response to Open Letter: Review of the Carcinogenicity of Glyphosate by EFSA and BfR*. URL: http://www.efsa.europa.eu/sites/default/files/EFSA_response_Prof_Portier.pdf (cit. on p. 64).

— (2015d). “The EFSA Data Warehouse access rules”. In: *EFSA supporting publication* (cit. on pp. 43, 85).

— (2015e). “The food classification and description system FoodEx 2 (revision 2)”. In: *EFSA Supporting Publications* 12.5, 804E (cit. on p. 48).

— (2016a). “Guidance on the preparation and presentation of an application for authorisation of a novel food in the context of Regulation (EU) 2015/2283”. In: *EFSA Journal* 14.11, e04594 (cit. on p. 52).

— (2016b). “Open risk assessment: data”. In: *EFSA Journal* 14, e00509 (cit. on p. 44).

— (2018c). *Shiny R tool for the automation of systematic reviews*. Version v4. URL: https://doi.org/10.5281/zenodo.1299740 (cit. on p. 56).

— (2018d). “Training on FoodEx2: Parma, 12-13 April 2018”. In: *EFSA Supporting Publications* 15.6, 1437E (cit. on p. 48).

— (2018e). “Use of EFSA Pesticide Residue Intake Model (EFSA PRIMo revision 3)”. In: *EFSA Journal* 16.1, e05147 (cit. on p. 56).

EFSA (2019a). *Chemical Monitoring Reporting Guidelines (SSD2)*. URL: https://doi.org/10.5281/zenodo.2543211 (cit. on p. 50).

— (2019b). "The raw primary commodity (RPC) model: strengthening EFSA's capacity to assess dietary exposure at different levels of the food chain, from raw primary commodities to foods as consumed". In: *EFSA Supporting Publications* 16.1, 1532E (cit. on pp. 45–47).

EFSA Panel on Dietetic Products, N. and A. (NDA) (2010). "Scientific opinion on establishing food-based dietary guidelines". In: *EFSA Journal* 8.3, p. 1460 (cit. on p. 61).

EFSA, S. Bronzwaer, G. Kass, T. Robinson, J. Tarazona, H. Verhagen, D. Verloo, D. Vrbos, and M. Hugas (2019). "Food safety regulatory research needs 2030". In: *EFSA Journal* 17.7, e170622 (cit. on p. 42).

EFSA, T. Donohoe, K. Garnett, A. O. Lansink, A. Afonso, and H. Noteborn (2018). "Emerging risks identification on food and feed–EFSA". In: *EFSA Journal* 16.7, e05359 (cit. on p. 54).

EFSA, B. Dujardin, and V. Bocca (2019). "Cumulative dietary exposure assessment of pesticides that have chronic effects on the thyroid using SAS® software". In: *EFSA Journal* 17.9, e05763 (cit. on pp. 57, 95, 136).

Eldridge, A., C. Piernas, A.-K. Illner, M. Gibney, M. Gurinović, J. de Vries, and J. Cade (2019). "Evaluation of new technology-based tools for dietary intake assessment—an ILSI Europe dietary intake and exposure task force evaluation". In: *Nutrients* 11.1, p. 55 (cit. on p. 52).

Ferentinos, K. P., C. P. Yialouris, P. Blouchos, G. Moschopoulou, and S. Kintzios (2013). "Pesticide residue screening using a novel artificial neural network combined with a bioelectric cellular biosensor". In: *BioMed research international* 2013 (cit. on p. 58).

Fischler, C. (1988). "Food, self and identity". In: *Information (International Social Science Council)* 27.2, pp. 275–292 (cit. on p. 62).

Floridi, L. (2010). *Information: A very short introduction*. OUP Oxford (cit. on p. 51).

— (2014). *The fourth revolution: How the infosphere is reshaping human reality*. OUP Oxford (cit. on pp. 7, 72).

Food Additives, E. P. on and N. S. added to Food (ANS) (2015). "Risk assessment for peri-and post-menopausal women taking food supplements containing isolated isoflavones". In: *EFSA Journal* 13.10, p. 4246 (cit. on p. 55).

Fossa, F. (2018). "Artificial moral agents: moral mentors or sensible tools?" In: *Ethics and Information Technology* 20.2, pp. 115–126 (cit. on p. 73).

— (2019). "«I Don't Trust You, You Faker!» On Trust, Reliance, and Artificial Agency". In: *Teoria. Rivista di filosofia* 39.1, pp. 63–80 (cit. on p. 73).

Fried, D., M. Surdeanu, S. Kobourov, M. Hingle, and D. Bell (2014). "Analyzing the language of food on social media". In: *2014 IEEE International Conference on Big Data (Big Data)*. IEEE, pp. 778–783 (cit. on p. 62).

Fritschi, L., J. McLaughlin, C. Sergi, G. Calaf, F. Le Curieux, F. Forastiere, H. Kromhout, P. Egeghy, G. Jahnke, C. Jameson, et al. (2015). "Carcinogenicity of tetrachlorvinphos, parathion, malathion, diazinon, and glyphosate". In: *Red* 114.2, pp. 70134–8 (cit. on p. 63).

Giabbanelli, P. and J. Adams (2016). "Identifying small groups of foods that can predict achievement of key dietary recommendations: data mining of the UK National Diet and Nutrition Survey, 2008–12". In: *Public health nutrition* 19.9, pp. 1543–1551 (cit. on p. 59).

Gilsenan, M. (2015). "Data handling: Observatories-databases-data storage-legal framework EFSA data collection". In: *Options Méditerranéennes. Series A: Mediterranean Seminars*. CIHEAM-IAMZ, Zaragoza (Spain)-EFSA, European Food Safety Authority, Parma (cit. on pp. 11, 43, 45, 50).

Gu, W., A. Vieira, R. Hoekstra, P. Griffin, and D. Cole (2015). "Use of random forest to estimate population attributable fractions from a case-control study of Salmonella enterica serotype Enteritidis infections". In: *Epidemiology and Infection* 143.13, pp. 2786–2794 (cit. on p. 58).

Hearty, A. P. and M. J. Gibney (2013). "Dietary patterns in Irish adolescents: a comparison of cluster and principal component analyses". In: *Public health nutrition* 16.5, pp. 848–857 (cit. on p. 59).

Hu, F. B. (2002). "Dietary pattern analysis: a new direction in nutritional epidemiology". In: *Current opinion in lipidology* 13.1, pp. 3–9 (cit. on p. 59).

IZSTO, G. Ru, M. Crescio, F. Ingravalle, C. Maurella, UBESP, D. Gregori, C. Lanera, D. Azzolina, G. Lorenzoni, et al. (2017). "Machine Learning Techniques applied in risk assessment related to food safety". In: *EFSA Supporting Publications* 14.7, 1254E (cit. on pp. 57, 58, 187, 211–213).

Jarschel, T., C. Laroque, R. Maschke, and P. Hartmann (2020). "Practical Classification and Evaluation of Optically Recorded Food Data by Using Various Big-Data Analysis Technologies". In: *Machines* 8.2, p. 34 (cit. on p. 51).

Jaspers, S., E. De Troyer, and M. Aerts (2018). "Machine learning techniques for the automation of literature reviews and systematic reviews in EFSA". In: *EFSA Supporting Publications* 15.6, 1427E (cit. on pp. 55, 56).

Jin, H., Y. Qin, H. Liang, L. Wan, H. Lan, G. Chen, R. Liu, L.-r. Zheng, P. Chiang, and Z.-l. Hong (2017). "A mobile-based high sensitivity on-field organophosphorus compounds detecting system for IoT-based food safety tracking". In: *Journal of Sensors* 2017 (cit. on p. 51).

Klaveren, J. D. van, J. W. Kruisselbrink, W. J. de Boer, G. van Donkersgoed, J. D. t. Biesebeek, M. Sam, and H. van der Voet (2019). "Cumulative dietary exposure assessment of pesticides that have chronic effects on the thyroid using MCRA software". In: *EFSA Supporting Publications* 16.9, 1707E (cit. on p. 57).

Kocharov, A. (2009). "Data ownership and access rights in the European Food Safety Authority". In: *European Food and Feed Law Review*, pp. 335–346 (cit. on pp. 44, 128, 130).

Lambe, J. (2002). "The use of food consumption data in assessments of exposure to food chemicals including the application of probabilistic modelling". In: *Proceedings of the Nutrition Society* 61.1, pp. 11–18 (cit. on p. 58).

Lazarou, C., M. Karaolis, A.-L. Matalas, and D. B. Panagiotakos (2012). "Dietary patterns analysis using data mining method. An application to data from the CYKIDS study". In: *Computer methods and programs in biomedicine* 108.2, pp. 706–714 (cit. on p. 59).

Lee, R. (2017). "Novel Foods and Risk Assessment in Europe". In: *The Oxford Handbook of Law, Regulation and Technology* (cit. on pp. 71, 77).

Lucas Luijckx, N. B., F. J. van de Brug, W. R. Leeman, J. M. van der Vossen, and H. J. Cnossen (2016). "Testing a text mining tool for emerging risk identification". In: *EFSA Supporting Publications* 13.12, 1154E (cit. on p. 55).

Maeda, Y., N. Kurita, and S. Ikeda (2005). "An early warning support system for food safety risks". In: *Annual Conference of the Japanese Society for Artificial Intelligence*. Springer, pp. 446–457 (cit. on p. 53).

Malgieri, G. and G. Comandé (2017). "Sensitive-by-distance: quasi-health data in the algorithmic era". In: *Information and Communications Technology Law* 26.3, pp. 229–249 (cit. on p. 61).

Maringer, M., P. van't Veer, N. Klepacz, M. C. Verain, A. Normann, S. Ekman, L. Timotijevic, M. M. Raats, and A. Geelen (2018). "User-documented food consumption data from publicly available apps: an analysis of opportunities and challenges for nutrition research". In: *Nutrition journal* 17.1, p. 59 (cit. on p. 52).

Marvin, H. J., E. M. Janssen, Y. Bouzembrak, P. J. Hendriksen, and M. Staats (2017). "Big data in food safety: An overview". In: *Critical Reviews in Food Science and Nutrition* 57.11, pp. 2286–2295 (cit. on pp. 7, 53).

Marvin, H. J., G. Kleter, A. Prandini, S. Dekkers, and D. Bolton (2009). "Early identification systems for emerging foodborne hazards". In: *Food and Chemical Toxicology* 47.5, pp. 915–926 (cit. on p. 55).

McHenry, L. B. (2018). "The Monsanto papers: poisoning the scientific well". In: *International Journal of Risk and Safety in Medicine* 29.3-4, pp. 193–205 (cit. on p. 64).

Mejova, Y., H. Haddadi, A. Noulas, and I. Weber (2015). "# foodporn: Obesity patterns in culinary interactions". In: *Proceedings of the 5th international conference on digital health 2015*. ACM, pp. 51–58 (cit. on p. 53).

Mittelstadt, B., P. Allo, M. Taddeo, S. Wachter, and L. Floridi (2016). "The ethics of algorithms: Mapping the debate". In: *Big Data & Society* 3.2, p. 2053951716679679 (cit. on p. 73).

Ocké, M., E. de Boer, H. Brants, J. van der Laan, M. Niekerk, C. van Rossum, L. Temme, H. Freisling, G. Nicolas, C. Casagrande, N. Slimani, E. Trolle, M. Ege, T. Christensen, S. Vandevijvere, M. Bellemans, M. De Maeyer, S. Defourny, J. Ruprich, M. Dofkova, I. Rehurkova, M. Jakubikova, J. Blahova, Z. Piskackova, and M. Maly (2012). "PANCAKE – Pilot study for the Assessment of Nutrient intake and food Consumption Among Kids in Europe". In: *EFSA Supporting Publications* 9.9, 339E. URL: `https://efsa.onlinelibrary.wiley.com/doi/abs/10.2903/sp.efsa.2012.EN-339` (cit. on p. 46).

Ortiz-Pelaez, Á. and D. U. Pfeiffer (2008). “Use of data mining techniques to investigate disease risk classification as a proxy for compromised biosecurity of cattle herds in Wales”. In: *BMC Veterinary Research* 4.1, p. 24 (cit. on p. 58).

PAN Europe (2020). *Fraud in German laboratory casts additional doubts on the 2017 re-approval of glyphosate and on the entire EU pesticide safety evaluation procedure*. https://www.pan-europe.info/press-releases/2020/02/fraud-german-laboratory-casts-additional-doubts-2017-re-approval-glyphosate. (Accessed on 03/02/2020) (cit. on p. 64).

Phan, T.-T., S. Muralidhar, and D. Gatica-Perez (2019). “Drinks & crowds: Characterizing alcohol consumption through crowdsensing and social media”. In: *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 3.2, pp. 1–30 (cit. on p. 53).

Portier, C. J. (2015). “Open letter: Review of the Carcinogenicity of Glyphosate by EChA, EFSA and BfR”. In: (cit. on p. 64).

Portier, C. J., B. K. Armstrong, B. C. Baguley, X. Baur, I. Belyaev, R. Bellé, F. Belpoggi, A. Biggeri, M. C. Bosland, P. Bruzzi, et al. (2016). “Differences in the carcinogenic evaluation of glyphosate between the International Agency for Research on Cancer (IARC) and the European Food Safety Authority (EFSA)”. In: *J Epidemiol Community Health* 70.8, pp. 741–745 (cit. on p. 64).

Rigdon, J. and S. Basu (2019). “Machine learning with sparse nutrition data to improve cardiovascular mortality risk prediction in the USA using nationally randomly sampled data”. In: *BMJ open* 9.11 (cit. on p. 59).

Rosso, N. and P. Giabbanelli (2018). “Accurately inferring compliance to five major food guidelines through simplified surveys: applying data mining to the UK National Diet and Nutrition Survey”. In: *JMIR public health and surveillance* 4.2, e56 (cit. on p. 59).

Rozin, P., L. Hammer, H. Oster, T. Horowitz, and V. Marmora (1986). “The child’s conception of food: differentiation of categories of rejected substances in the 16 months to 5 year age range”. In: *Appetite* 7.2, pp. 141–151 (cit. on p. 61).

Russell, S. and P. Norvig (2010). “Artificial intelligence: a modern approach”. In: (cit. on pp. 17, 18, 57, 154).

Sapienza, S. and M. Palmirani (2018). “Emerging data governance issues in big data applications for food safety”. In: *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (cit. on p. 51).

Sasahara, K. (2018). “You are what you eat: A social media study of food identity”. In: *arXiv preprint arXiv:1808.08428* (cit. on p. 62).

Sharma, S. S. and M. De Choudhury (2015). “Measuring and characterizing nutritional information of food and ingestion content in instagram”. In: *Proceedings of the 24th International Conference on World Wide Web*. ACM, pp. 115–116 (cit. on p. 53).

Soon, J. M. and I. S. Saguy (2017). “Crowdsourcing: A new conceptual view for food safety and quality”. In: *Trends in food science and technology* 66, pp. 63–72 (cit. on p. 51).

Strawn, L. K., E. D. Fortes, E. A. Bihn, K. K. Nightingale, Y. T. Gröhn, R. W. Worobo, M. Wiedmann, and P. W. Bergholz (2013). "Landscape and meteorological factors affecting prevalence of three food-borne pathogens in fruit and vegetable farms". In: *Appl. Environ. Microbiol.* 79.2, pp. 588–600 (cit. on p. 58).

Taddeo, M. (2017). "Trusting digital technologies correctly". In: *Minds and Machines* 27.4, pp. 565–568 (cit. on pp. 73, 169).

Taddeo, M. and L. Floridi (2018). "How AI can be a force for good". In: *Science* 361.6404, pp. 751–752 (cit. on p. 73).

Tao, D., P. Yang, and H. Feng (2020). "Utilization of text mining as a big data analysis tool for food science and nutrition". In: *Comprehensive Reviews in Food Science and Food Safety* 19.2, pp. 875–894 (cit. on pp. 55, 56).

The Guardian (2017). *EU report on weedkiller safety copied text from Monsanto study | Environment | The Guardian*. https://www.theguardian.com/environment/2017/sep/15/eu-report-on-weedkiller-safety-copied-text-from-monsanto-study. (Accessed on 03/02/2020) (cit. on p. 64).

Thompson, F. E., A. F. Subar, C. M. Loria, J. L. Reedy, and T. Baranowski (2010). "Need for technological innovation in dietary assessment". In: *Journal of the Academy of Nutrition and Dietetics* 110.1, pp. 48–51 (cit. on p. 52).

Van den Puttelaar, J., M. C. Verain, and M. C. Onwezen (2016). "The potential of enriching food consumption data by use of consumer generated data: A case from RICHFIELDS". In: *Proceedings of Measuring Behavior 2016* (cit. on p. 52).

Yakovlev, P. A. and W. P. Guessford (2013). "Alcohol consumption and political ideology: What's party got to do with it?" In: *Journal of Wine Economics* 8.3, pp. 335–354 (cit. on p. 62).

Zhao, G., Y. Guo, X. Sun, and X. Wang (2015). "A system for pesticide residues detection and agricultural products traceability based on acetylcholinesterase biosensor and internet of things". In: *International Journal of Electrochemical Science* 10.4, pp. 3387–3399 (cit. on p. 51).

References for Chapter 3: EU Food Law and Policy on Openness and Transparency of data

Alemanno, A. (2011). "Annotation of European Court of Justice, Case C-79/09, Gowan Comércio Internacional E Serviços Lda V. Ministero Della Salute (Precautionary Principle)". In: (cit. on p. 110).

— (2014). "Unpacking the principle of openness in EU law: transparency, participation and democracy". In: *European Law Review* (cit. on pp. 7, 124, 126).

Alemanno, A. and S. Gabbi (2016). *Foundations of EU food law and policy: Ten years of the European food safety authority*. Routledge (cit. on pp. 2, 4, 42, 47, 61, 62, 79, 125, 131, 140, 141).

Aplin, T. and J. Davis (2013). *Intellectual property law: text, cases, and materials*. Oxford University Press (cit. on pp. 129, 130).

Bartl, A. (2015). "REFIT of food legislation: An opportunity to discuss implementation and enforcement issues". In: *European Food and Feed Law Review*, pp. 84–91 (cit. on p. 86).

Bazylińska-Nagler, J. (2017). "The Right of Access to Environmental Information in the Light of the Case C-673/13 P of 23 November 2016—European Commission V Stichting Greenpeace Nederland". In: *Wroclaw Review of Law, Administration & Economics* 7.2, pp. 66–82 (cit. on pp. 112, 113).

Bernauer, T., T. Tribaldos, C. Luginbühl, and M. Winzeler (2011). "Government regulation and public opposition create high additional costs for field trials with GM crops in Switzerland". In: *Transgenic research* 20.6, pp. 1227–1234 (cit. on p. 98).

Berthier, A. (2016). "Transparency in EU law-making". In: *ERA Forum*. Vol. 17. 4. Springer, pp. 423–436 (cit. on p. 117).

Beversdorf, D. Q., R. P. Roos, W. A. Hauser, V. A. Lennon, and M. F. Mehler (2015). "Animal extremists' threats to neurologic research continue: neuroreality II". In: *Neurology* 85.8, pp. 730–734 (cit. on p. 94).

Borghi, M. and S. Karapapa (2015). "Contractual Restrictions on Lawful Use of Information: Sole-Source Databases Protected by the Back Door?" In: *EIPR* 37.8, pp. 505–514 (cit. on p. 130).

Buonsante, V. A. and A. Friel (2017). "What is Information Relating to Emissions into the Environment?" In: *European Journal of Risk Regulation* 8.2, pp. 453–460 (cit. on p. 114).

Conte-Salinas, N. and R. Wallau (2016). "The Concepts of Transparency and Openness in European Food Law". In: *International Food Law and Policy*. Springer, pp. 581–606 (cit. on p. 125).

De Minico, G. (2019). "Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria". In: *Diritto pubblico* 25.1, pp. 89–116 (cit. on p. 140).

De Montjoye, Y.-A., C. A. Hidalgo, M. Verleysen, and V. D. Blondel (2013). "Unique in the crowd: The privacy bounds of human mobility". In: *Scientific reports* 3, p. 1376 (cit. on p. 138).

DECODE project (2020). *Common Knowledge: Citizen-led data governance for better cities*. URL: https://decodeproject.eu/publications/common-knowledge-citizen-led-data-governance-better-cities (cit. on pp. 22, 24, 135).

Dubuisson, C., S. Carrillo, A. Dufour, S. Havard, P. Pinard, and J.-L. Volatier (2017). "The French dietary survey on the general population (INCA3)". In: *EFSA Supporting Publications* 14.12 (cit. on p. 96).

Durante, M. (2019). *Potere computazionale: L'impatto delle ICT su diritto, società, sapere*. Mimesis (cit. on pp. 7, 125, 184).

EFSA (2006). "Opinion of the Scientific Panel on Animal Health and Welfare (AHAW) on request from the European Commission related to: Assessing the risk of Foot and Mouth Disease introduction into the EU from developing countries, assessing the reduction of this risk through interventions in developing countries/regions aiming at controlling/eradicating the disease, and Tools for the control of a Foot and Mouth Disease outbreak: update on diagnostics and vaccines". In: *EFSA Journal* 4.2, p. 313 (cit. on p. 77).

EFSA (2014a). "Guidance on the EU Menu methodology". In: *EFSA Journal* 12.12, p. 3944 (cit. on pp. 46, 96).

— (2015d). "The EFSA Data Warehouse access rules". In: *EFSA supporting publication* (cit. on pp. 43, 85).

— (2017). "Safety of cranberry extract powder as a novel food ingredient pursuant to Regulation (EC) No 258/97". In: *EFSA Journal* 15.5, e04777 (cit. on p. 108).

— (2018a). "Administrative guidance for the processing of applications for regulated products (update 2019)". In: *EFSA Supporting Publications* 15.1, 1362E (cit. on p. 84).

— (2018b). *EU MENU Structural Metadata*. EU; CSV; data.collection@efsa.europa.eu. URL: https://doi.org/10.5281/zenodo.1215993 (cit. on pp. 136, 214).

— (2020). *EFSA Programming Document 2020 - 2022*. http://www.efsa.europa.eu/sites/default/files/corporate_publications/files/amp2022.pdf. (Accessed on 05/15/2020) (cit. on p. 123).

EFSA, B. Dujardin, and V. Bocca (2019). "Cumulative dietary exposure assessment of pesticides that have chronic effects on the thyroid using SAS® software". In: *EFSA Journal* 17.9, e05763 (cit. on pp. 57, 95, 136).

EFSA, H. Naegeli, A. N. Birch, J. Casacuberta, A. De Schrijver, M. A. Gralak, P. Guerche, H. Jones, B. Manachini, A. Messéan, et al. (2018). "Assessment of genetically modified maize 4114 for food and feed uses, under Regulation (EC) No 1829/2003 (application EFSA-GMO-NL-2014-123)". In: *EFSA Journal* 16.5, e05280 (cit. on p. 99).

European Commission (2020). *Commission White Paper on Artificial Intelligence - A European approach to excellence and trust*. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. (Accessed on 05/22/2020) (cit. on pp. 18, 140, 148, 151, 182, 184, 186, 192).

Faini, F. and M. Palmirani (2018). "The Right to Know and Digital Technology: Proactive and Reactive Transparency in the Italian Legal System". In: *International Conference on Electronic Government and the Information Systems Perspective*. Springer, pp. 164–174 (cit. on p. 80).

Floridi, L. (2005). "The ontological interpretation of informational privacy". In: *Ethics and Information Technology* 7.4, pp. 185–200 (cit. on pp. 23, 134, 193).

Gabbi, S. (2008). "The European Food Safety Authority: judicial review by community courts". In: *Revue européenne de droit de la consommation (REDC)-European Journal of Consumer Law* 1.2009, pp. 171–189 (cit. on p. 141).

Holle, M. (2014). "The Protection of Proprietary Data in Novel Foods–How to Make It Work". In: *European Food and Feed Law Review*, pp. 280–284 (cit. on pp. 100, 129).

Holleben, H. von (2013). “Judgment of the General Court of the EU on Access to Information under Substance Law: Case T-545/11, Judgment of 08 October 2013”. In: *European Journal of Risk Regulation* 4.4, pp. 565–578 (cit. on pp. 112, 113).

Jaeger, M. (2019). *Access to file & confidentiality - the role of the Court of Justice of the European Union*. (Accessed on 05/08/2020) (cit. on p. 120).

Jasanoff, S. (2016). *The ethics of invention: technology and the human future*. WW Norton & Company (cit. on pp. 77, 98).

Knowles, T., R. Moody, and M. G. McEachern (2007). “European food scares and their impact on EU food policy”. In: *British food journal* (cit. on p. 76).

Kocharov, A. (2009). “Data ownership and access rights in the European Food Safety Authority”. In: *European Food and Feed Law Review*, pp. 335–346 (cit. on pp. 44, 128, 130).

Korkea-Aho, E. and P. Leino (2017). “Who owns the information held by EU agencies? Weed killers, commercially sensitive information and transparent and participatory governance”. In: *Common Market Law Review* 54.4, pp. 1059–1091 (cit. on pp. 111, 118, 131).

Lee, R. (2017). “Novel Foods and Risk Assessment in Europe”. In: *The Oxford Handbook of Law, Regulation and Technology* (cit. on pp. 71, 77).

Lodge, J. (2003). “Transparency and EU Governance: Balancing Openness with Security”. In: *Journal of Contemporary European Studies* 11.1, pp. 95–117 (cit. on p. 124).

Lok, C. and D. Powell (2000). “The Belgian Dioxin Crisis of the Summer of 1999: a case study in crisis communications and management”. In: (cit. on p. 77).

Lynch, M. P. (2016). *The internet of us: Knowing more and understanding less in the age of big data*. WW Norton & Company (cit. on pp. 125, 187).

Malgieri, G. (2016). “’Ownership’of Customer (Big) Data in the European Union: Quasi-Property as Comparative Solution?” In: *Journal of Internet Law* 20.5 (cit. on p. 134).

Marcos, S. V., M. J. Rubio, F. R. Sanchidrián, and D. de Robledo (2016). “Spanish National dietary survey in adults, elderly and pregnant women”. In: *EFSA Supporting Publications* 13.6 (cit. on p. 96).

Martuzzi, M., J. A. Tickner, et al. (2004). *The precautionary principle: protecting public health, the environment and the future of our children* (cit. on p. 78).

McDougall, P. (2011). “The cost and time involved in the discovery, development and authorisation of a new plant biotechnology derived trait”. In: *Crop Life International*, pp. 1–24 (cit. on p. 98).

Mittelstadt, B., C. Russell, and S. Wachter (2019). “Explaining explanations in AI”. In: pp. 279–288 (cit. on pp. 140, 186, 190).

Morvillo, M. (2019). “The General Court Orders Disclosure of Glyphosate-related Scientific Studies: Tweedale, Hautala, and the Concept of Environmental Information in the Context of Plant Protection Products”. In: *European Journal of Risk Regulation* 10.2, pp. 419–427 (cit. on pp. 116, 117).

Moules, R. (2017). “Significant EU environmental cases: 2016”. In: *Journal of Environmental Law* 29.1, pp. 177–188 (cit. on pp. 111, 113, 114).

Peel, J. (2012). “Of Apples and Oranges (and Hormones in Beef): Science and the Standard of Review in WTO Disputes under the SPS Agreement”. In: *International & Comparative Law Quarterly* 61.2, pp. 427–458 (cit. on p. 110).

Public Health, N. I. for, the Environment, C. van Rossum, K. Nelis, C. Wilson, and M. Ocké (2018). “National dietary survey in 2012-2016 on the general population aged 1-79 years in the Netherlands”. In: *EFSA Supporting Publications* 15.9, 1488E (cit. on p. 96).

Rifkin, J. and T. Howard (1977). “Who should play God?” In: *The Progressive* 41.12, pp. 16–22 (cit. on p. 98).

Rusconi, G. (2016). “Food Safety and Policy in the European Union”. In: *International Food Law and Policy*. Springer, pp. 451–483 (cit. on pp. 11, 80, 81, 110).

Sachs, G. (2016). “Introduction to European food law and regulation”. In: *International Food Law and Policy*. Springer, pp. 409–450 (cit. on pp. 97, 104, 105).

Sapienza, S. (2019). *Transparency and Openness in Food Safety: insights about new Data Confidentiality rules*. URL: https://doi.org/10.5281/zenodo.2766359 (cit. on p. 123).

Schleissing, S., S. Pfeilmeier, and C. Dürnberger (2019). *Genome Editing in Agriculture: Between Precaution and Responsibility*. Nomos Verlag (cit. on p. 98).

Sette, S., C. Le Donne, R. Piccinelli, D. Arcella, A. Turrini, C. Leclercq, I.-S. 2.-.-.-0. S. Group, et al. (2011). “The third Italian national food consumption survey, INRAN-SCAI 2005–06–part 1: nutrient intakes in Italy”. In: *Nutrition, Metabolism and Cardiovascular Diseases* 21.12, pp. 922–932 (cit. on p. 96).

Simpson, C. (2016). “Data Protection under Food Law Post: in the Aftermath of the Novel Foods Regulation”. In: *Eur. Food & Feed L. Rev.* 11, p. 309 (cit. on pp. 5, 100, 129, 130).

Tamò-Larrieux, A. (2018). “Mapping the Privacy Rationales”. In: *Designing for Privacy and its Legal Framework*. Springer, pp. 27–43 (cit. on pp. 23, 134).

Vos, E. (2000). “EU food safety regulation in the aftermath of the BSE crisis”. In: *Journal of consumer policy* 23.3, pp. 227–255 (cit. on p. 77).

References for Chapter 4: The ethical perspective: AI Ethics initiatives and charters for a trustworthy innovation

AGID, A. p. L. D. (2018). *Libro Bianco sull’Intelligenza Artificiale al servizio del cittadino*. https://libro-bianco-ia.readthedocs.io/en/latest/. (Accessed on 02/11/2020) (cit. on pp. 157, 181, 190, 192).

AI4People (2018). *AI4People | Atomium*. URL: https://www.eismd.eu/ai4people/ (cit. on pp. 37, 147, 186, 189).

Aplin, T. (2020). *Research Handbook on Intellectual Property and Digital Technologies*. Research Handbooks in Intellectual Property series. Edward Elgar Publishing Limited. URL: https://books.google.it/books?id=jf3LDwAAQBAJ (cit. on p. 171).

Balkin, J. M. (2017). “Free speech in the algorithmic society: Big data, private governance, and new school speech regulation”. In: *UCDL Rev.* 51, p. 1149 (cit. on p. 168).

Bart, V. (2020). “Artificial intelligence as law”. In: *Artificial Intelligence and Law* 28.2, pp. 181–206 (cit. on p. 157).

Beauchamp, T. L., J. F. Childress, et al. (2001). *Principles of biomedical ethics*. Oxford University Press, USA (cit. on p. 170).

Bietti, E. (2020). “From ethics washing to ethics bashing: a view on tech ethics from within moral philosophy”. In: *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, pp. 210–219 (cit. on pp. 167, 168).

BMWi, G. F. M. f. E. A. (2018). *Artificial Intelligence Strategy*. https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2018/20180718-key-points-for-federal-government-strategy-on-artificial-intelligence.html. (Accessed on 02/11/2020) (cit. on pp. 148, 154, 180, 182, 186, 190, 192).

Calo, R. (2017). “Artificial Intelligence policy: a primer and roadmap”. In: *UCDL Rev.* 51, p. 399 (cit. on p. 167).

European Commission (2018). *Communication Artificial Intelligence for Europe*. https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe. (Accessed on 02/11/2020) (cit. on pp. 151, 186).

— (2020). *Commission White Paper on Artificial Intelligence - A European approach to excellence and trust*. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. (Accessed on 05/22/2020) (cit. on pp. 18, 140, 148, 151, 182, 184, 186, 192).

Fjeld, J., N. Achten, H. Hilligoss, A. Nagy, and M. Srikumar (2020). “Principled Artificial Intelligence: Mapping Consensus in Ethical and Rights-based Approaches to Principles for AI”. In: *Berkman Klein Center Research Publication* 2020-1 (cit. on pp. 147, 167).

Floridi, L. (2013a). *The ethics of information*. Oxford University Press (cit. on pp. 162, 170, 192).

— (2018). “Soft Ethics and the Governance of the Digital”. In: *Philosophy and Technology* 31.1, pp. 1–8 (cit. on pp. 7, 149).

— (2019b). “Translating principles into practices of digital ethics: Five risks of being unethical”. In: *Philosophy & Technology* 32.2, pp. 185–193 (cit. on p. 166).

Floridi, L. and J. Cowls (2019). “A unified framework of five principles for AI in society”. In: *Harvard Data Science Review* (cit. on p. 147).

Floridi, L., J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo, F. Rossi, et al. (2018). “AI4People—An ethical framework for a good AI society: opportunities, risks, principles, and recommendations”. In: *Minds and Machines* 28.4, pp. 689–707 (cit. on pp. 37, 162).

Future of Life Institute (2017). “Principles developed in conjunction with the 2017 Asilomar conference”. In: *Principles developed in conjunction with the 2017 Asilomar conference [Benevolent AI 2017]* (cit. on p. 159).

Hagendorff, T. (2020). “The ethics of Ai ethics: An evaluation of guidelines”. In: *Minds and Machines*, pp. 1–22 (cit. on p. 147).

Hart, H. L. A. (1961). *The Concept of Law*. Oxford university press (cit. on p. 173).

HLEG, H. L. E. G. o. A. (2019). “Ethics guidelines for trustworthy AI”. In: *B-1049 Brussels* (cit. on pp. 163, 180, 182, 184, 186, 188, 190).

IEEE (2017). “Ethically aligned design”. In: *IEEE Standards v2* (cit. on pp. 161, 169).

Jobin, A., M. Ienca, and E. Vayena (2019). “The global landscape of AI ethics guidelines”. In: *Nature Machine Intelligence* 1.9, pp. 389–399 (cit. on pp. 147, 167, 184, 189).

Kuner, C., F. H. Cate, O. Lynskey, C. Millard, N. Ni Loideain, and D. J. B. Svantesson (2018). *Expanding the artificial intelligence-data protection debate* (cit. on p. 153).

Lessig, L. (2009). *Code: And other laws of cyberspace* (cit. on p. 173).

Mantelero, A. (2020). *Analysis of the International legally binding instruments*. `https://rm.coe.int/cahai-2020-08-fin-mantelero-binding-instruments-report-2020-def/16809eca33`. (Accessed on 07/07/2020) (cit. on pp. 149, 174).

Mittelstadt, B. (2019). “AI Ethics–Too Principled to Fail?” In: *arXiv preprint arXiv:1906.06668* (cit. on pp. 148, 170, 171).

Morley, J., L. Floridi, L. Kinsey, and A. Elhalal (2019). “From What to How: An Initial Review of Publicly Available AI Ethics Tools, Methods and Research to Translate Principles into Practices”. In: *Science and Engineering Ethics*, pp. 1–28 (cit. on pp. 147, 148, 167).

Nabi, J. (2018). “How bioethics can shape artificial intelligence and machine learning”. In: *Hastings Center Report* 48.5, pp. 10–13 (cit. on p. 171).

Pagallo, U., P. Casanovas, and R. Madelin (2019). “The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data”. In: *The Theory and Practice of Legislation*, pp. 1–25 (cit. on pp. 27, 30, 147, 152, 167, 172, 183).

Pavon, J. and M. Gonzalez-Espejo (2020). *An Introductory Guide to Artificial Intelligence for Legal Professionals*. Wolters Kluwer (cit. on p. 151).

Quintarelli, S., F. Corea, F. Fossa, A. Loreggia, and S. Sapienza (2019). “Una prospettiva etica sull’Intelligenza Artificiale: principi, diritti e raccomandazioni”. In: (cit. on p. 153).

Renda, A. et al. (2019). *Artificial Intelligence*. CEPS Centre for European Policy Studies (cit. on p. 170).

Russell, S. and P. Norvig (2010). “Artificial intelligence: a modern approach”. In: (cit. on pp. 17, 18, 57, 154).

Ryan, M. and B. C. Stahl (2020). “Artificial intelligence ethics guidelines for developers and users: clarifying their content and normative implications”. In: *Journal of Information, Communication and Ethics in Society* (cit. on p. 157).

SIGAI, T. S. I. G. o. A. (2019). *Dutch AI Manifesto*. http://ii.tudelft.nl/bnvki/wp-content/uploads/2019/09/Dutch-AI-Manifesto-2019.pdf. (Accessed on 02/11/2020) (cit. on pp. 156, 182, 184, 190).

Smit, K., M. Zoet, and J. van Meerten (2020). "A Review of AI Principles in Practice". In: (cit. on pp. 148, 169).

Taddeo, M. (2017). "Trusting digital technologies correctly". In: *Minds and Machines* 27.4, pp. 565–568 (cit. on pp. 73, 169).

Tallacchini, M. (2015). "To bind or not bind? European ethics as soft law: European ethics as soft law Mariachiara Tallacchini". In: *Science and Democracy*. Routledge, pp. 174–193 (cit. on p. 149).

Van Dijk, N. and S. Casiraghi (Mar. 2020). *The "ethification" of privacy and data protection in the EU. The case of Artificial Intelligence, Privacy Hub Working Paper. Vol. 6, Nr. 22 (May), 2020,* (cit. on p. 149).

Villani, C., Y. Bonnet, B. Rondepierre, et al. (2018). *For a meaningful artificial intelligence: Towards a French and European strategy*. Conseil national du numérique (cit. on pp. 148, 155, 182, 183, 188, 190, 192).

Wagner, B. (2018). "Ethics as an escape from regulation: From ethics-washing to ethics-shopping". In: (cit. on pp. 166, 167).

References for Chapter 5: A Principle-Based Roadmap for Food Safety Datafication: The P-SAFETY model

AGID, A. p. L. D. (2018). *Libro Bianco sull'Intelligenza Artificiale al servizio del cittadino*. https://libro-bianco-ia.readthedocs.io/en/latest/. (Accessed on 02/11/2020) (cit. on pp. 157, 181, 190, 192).

AI4People (2018). *AI4People | Atomium*. URL: https://www.eismd.eu/ai4people/ (cit. on pp. 37, 147, 186, 189).

Alexy, R. (2000). "On the structure of legal principles". In: *Ratio juris* 13.3, pp. 294–304 (cit. on p. 179).

— (2003). "On balancing and subsumption. A structural comparison". In: *Ratio Juris* 16.4, pp. 433–449 (cit. on p. 179).

Barocas, S. and A. D. Selbst (2016). "Big data's disparate impact". In: *Calif. L. Rev.* 104, p. 671 (cit. on p. 185).

BMWi, G. F. M. f. E. A. (2018). *Artificial Intelligence Strategy*. https://www.bmwi.de/Redaktion/EN/Pressemitteilungen/2018/20180718-key-points-for-federal-government-strategy-on-artificial-intelligence.html. (Accessed on 02/11/2020) (cit. on pp. 148, 154, 180, 182, 186, 190, 192).

Cowls, J., T. King, M. Taddeo, and L. Floridi (2019). "Designing AI for social good: Seven essential factors". In: *Available at SSRN 3388669* (cit. on p. 189).

De Hert, P. (2017). "Data protection as bundles of principles, general rights, concrete subjective rights and rules: piercing the veil of stability surrounding the principles of data protection". In: *Eur. Data Prot. L. Rev.* 3, pp. 160–179 (cit. on pp. 193, 194).

Doshi-Velez, F. and B. Kim (2017). “Towards a rigorous science of interpretable machine learning”. In: *arXiv preprint arXiv:1702.08608* (cit. on p. 188).

Doshi-Velez, F., M. Kortz, R. Budish, C. Bavitz, S. Gershman, D. O’Brien, S. Schieber, J. Waldo, D. Weinberger, and A. Wood (2017). “Accountability of AI under the law: The role of explanation”. In: *arXiv preprint arXiv:1711.01134* (cit. on pp. 186, 188).

Durante, M. (2019). *Potere computazionale: L’impatto delle ICT su diritto, società, sapere*. Mimesis (cit. on pp. 7, 125, 184).

Dwork, C., M. Hardt, T. Pitassi, O. Reingold, and R. Zemel (2012). “Fairness through awareness”. In: *Proceedings of the 3rd innovations in theoretical computer science conference*, pp. 214–226 (cit. on pp. 185, 186).

European Commission (2018). *Communication Artificial Intelligence for Europe*. https://ec.europa.eu/digital-single-market/en/news/communication-artificial-intelligence-europe. (Accessed on 02/11/2020) (cit. on pp. 151, 186).

— (2020). *Commission White Paper on Artificial Intelligence - A European approach to excellence and trust*. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf. (Accessed on 05/22/2020) (cit. on pp. 18, 140, 148, 151, 182, 184, 186, 192).

Feteris, E. T., Feteris, and Olivier (2017). *Fundamentals of legal argumentation*. Vol. 1. Springer (cit. on p. 180).

Floridi, L. (2005). “The ontological interpretation of informational privacy”. In: *Ethics and Information Technology* 7.4, pp. 185–200 (cit. on pp. 23, 134, 193).

— (2013a). *The ethics of information*. Oxford University Press (cit. on pp. 162, 170, 192).

— (2017). “Group privacy: A defence and an interpretation”. In: *Group Privacy*. Springer, pp. 83–100 (cit. on p. 194).

González, E. G. and P. de Hert (2019). “Understanding the legal provisions that allow processing and profiling of personal data — an analysis of GDPR provisions and principles”. In: *Era Forum*. Vol. 19. 4. Springer, pp. 597–621 (cit. on p. 195).

Hacker, P. (2018). “Teaching fairness to artificial intelligence: Existing and novel strategies against algorithmic discrimination under EU law”. In: (cit. on pp. 184, 194).

Hallinan, D. and P. de Hert (2017). “Genetic classes and genetic categories: protecting genetic groups through data protection law”. In: *Group Privacy*. Springer, pp. 175–196 (cit. on p. 185).

HLEG, H. L. E. G. o. A. (2019). “Ethics guidelines for trustworthy AI”. In: *B-1049 Brussels* (cit. on pp. 163, 180, 182, 184, 186, 188, 190).

ICO (2018). *Accountability and governance*. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/. (Accessed on 07/29/2020) (cit. on p. 194).

IZSTO, G. Ru, M. Crescio, F. Ingravalle, C. Maurella, UBESP, D. Gregori, C. Lanera, D. Azzolina, G. Lorenzoni, et al. (2017). "Machine Learning Techniques applied in risk assessment related to food safety". In: *EFSA Supporting Publications* 14.7, 1254E (cit. on pp. 57, 58, 187, 211–213).

Jobin, A., M. Ienca, and E. Vayena (2019). "The global landscape of AI ethics guidelines". In: *Nature Machine Intelligence* 1.9, pp. 389–399 (cit. on pp. 147, 167, 184, 189).

Kamishima, T., S. Akaho, H. Asoh, and J. Sakuma (2012). "Considerations on fairness-aware data mining". In: *2012 IEEE 12th International Conference on Data Mining Workshops*. IEEE, pp. 378–385 (cit. on p. 186).

Lynch, M. P. (2016). *The internet of us: Knowing more and understanding less in the age of big data*. WW Norton & Company (cit. on pp. 125, 187).

Lynskey, O. (2014). "Deconstructing data protection: The added-value of a right to data protection in the EU legal order". In: *Int'l & Comp. LQ* 63, p. 569 (cit. on p. 193).

Mittelstadt, B., C. Russell, and S. Wachter (2019). "Explaining explanations in AI". In: pp. 279–288 (cit. on pp. 140, 186, 190).

Olivier, M. S. (2002). "Database privacy: balancing confidentiality, integrity and availability". In: *ACM SIGKDD Explorations Newsletter* 4.2, pp. 20–27 (cit. on p. 181).

Pagallo, U. (2020). "Algoritmi e conoscibilità". In: *Rivista di filosofia del diritto* 9.1, pp. 93–106 (cit. on p. 188).

Pagallo, U., P. Casanovas, and R. Madelin (2019). "The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data". In: *The Theory and Practice of Legislation*, pp. 1–25 (cit. on pp. 27, 30, 147, 152, 167, 172, 183).

Palmirani, M. (2020). "Big Data e conoscenza". In: *Rivista di filosofia del diritto* 9.1, pp. 73–92 (cit. on pp. 188, 190, 193, 195).

Rawls, J. (2009). *A theory of justice*. Harvard university press (cit. on p. 186).

Sabelli, C. and M. Tallacchini (2017). "From privacy to algorithms' fairness". In: *IFIP International Summer School on Privacy and Identity Management*. Springer, pp. 86–110 (cit. on pp. 186, 194).

SIGAI, T. S. I. G. o. A. (2019). *Dutch AI Manifesto*. http://ii.tudelft.nl/bnvki/wp-content/uploads/2019/09/Dutch-AI-Manifesto-2019.pdf. (Accessed on 02/11/2020) (cit. on pp. 156, 182, 184, 190).

Tallacchini, M. (2014). "Between Uncertainty and Responsibility: precaution and the complex journey towards reflexive innovation". In: (cit. on p. 188).

Vedder, A. (2019). "Safety, Security and Ethics". In: *Anton Vedder, Safety, Security and Ethics. In: Anton Vedder, Jessica Schroers, Charlotte Ducuing & Peggy Valcke (eds), Security and Law. Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security. Cambridge, Antwerp, Chicago: Intersentia*, pp. 11–26 (cit. on p. 180).

Vedder, A. and L. Naudts (2017). “Accountability for the use of algorithms in a big data environment”. In: *International Review of Law, Computers & Technology* 31.2, pp. 206–224 (cit. on pp. 183, 184).

Villani, C., Y. Bonnet, B. Rondepierre, et al. (2018). *For a meaningful artificial intelligence: Towards a French and European strategy*. Conseil national du numérique (cit. on pp. 148, 155, 182, 183, 188, 190, 192).

Wachter, S., B. Mittelstadt, and L. Floridi (2017). “Why a right to explanation of automated decision-making does not exist in the general data protection regulation”. In: *International Data Privacy Law* 7.2, pp. 76–99 (cit. on pp. 188, 195).

Wachter, S., B. Mittelstadt, and C. Russell (2017). “Counterfactual explanations without opening the black box: Automated decisions and the GDPR”. In: *Harv. JL & Tech.* 31, p. 841 (cit. on p. 190).

Zarsky, T. (2016). “The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making”. In: *Science, Technology, & Human Values* 41.1, pp. 118–132 (cit. on p. 186).

References for Chapter 6: Final remarks and future research

Sacco, R. (1991). “Legal formants: a dynamic approach to comparative law (Installment I of II)”. In: *The American Journal of Comparative Law* 39.1, pp. 1–34 (cit. on pp. 34, 203).

Savonitto, G. (2019). *Pharmaceuticals in the European Union: Law and Economics*. Cambridge Scholars Publishing (cit. on p. 206).

References for Chapter 6.3: Appendix

EFSA (2018b). *EU MENU Structural Metadata*. EU; CSV; data.collection@efsa.europa.eu. URL: https://doi.org/10.5281/zenodo.1215993 (cit. on pp. 136, 214).

IZSTO, G. Ru, M. Crescio, F. Ingravalle, C. Maurella, UBESP, D. Gregori, C. Lanera, D. Azzolina, G. Lorenzoni, et al. (2017). “Machine Learning Techniques applied in risk assessment related to food safety”. In: *EFSA Supporting Publications* 14.7, 1254E (cit. on pp. 57, 58, 187, 211–213).

Quo pertinet haec dicere? Ut appareat contemplationem placere omnibus; alii petunt illam, nobis haec statio, non portus est

Seneca, de Otio