Journal of Responsible Technology 10 (2022) 100028

Contents lists available at ScienceDirect

Journal of Responsible Technology

journal homepage: www.sciencedirect.com/journal/journal-of-responsible-technology

Business and human rights in Industry 4.0: A blueprint for collaborative human rights due diligence in the Factories of the Future☆

Ivo Emanuilov [a,*], Katerina Yordanova [b]

[a] Centre for IT & IP Law at KU Leuven, 6 Sint-Michielsstraat, MTC 03.25, Leuven, 3000, Belgium
[b] Centre for IT & IP Law at KU Leuven, 6 Sint-Michielsstraat, MTC 04.24, Leuven, 3000, Belgium

ARTICLE INFO

Keywords:
Industry 4.0
Smart manufacturing
Human rights
Collaborative due diligence

ABSTRACT

The digitalisation of production driven by new paradigms such as Industry 4.0, factories of the future and smart manufacturing, create new challenges as to how manufacturers and other supply chain actors would discharge their corporate responsibility to respect human rights. These new paradigms enable novel approaches like distributed and collaborative manufacturing. Manufacturers increasingly leverage digital technologies, such as 3D printing, cloud manufacturing and artificial intelligence, to provide customised products. Digital technologies also improve predictive and preventive maintenance on the shop floor and across the supply chain, increasing the overall resilience of manufacturing industries in times of crisis. This article proposes a blueprint of a collaborative, decentralised approach to human rights due diligence in digital supply chains. It argues that the pooling of human rights due diligence efforts in manufacturing industries could have network-wide effects of incentivising value chain actors to also collaborate on providing collective remedy.

1. Introduction

The manufacturing of a modern aircraft, like an Airbus A321, is the result of highly efficient cooperation across complex, tightly integrated global supply and manufacturing chains. The process starts with the design and engineering, through production and transport of aircraft sections, to final assembly and tests, certification and delivery to the customer. Growing demand in air travel in the past few decades has naturally increased the production needs. At the same time, fast-paced developments in the information and communications technology (ICT) industry have offered new ways of optimising manufacturing. As a result, the supply chain of modern aircraft production no longer consists of just raw materials, such as steel, aluminium, titanium and their alloys. The deployment of smart sensors on the shop floor and the utilization of automated systems means that supply chains now include also *digital* assets, such as datasets, computer simulations, digital twins and pre-trained machine learning models.

New models of manufacturing are enabled by concepts like distributed, collaborative and additive manufacturing. At the same time, they also create distinct challenges as to how manufacturers and the various actors in their supply chains could discharge their corporate responsibility to respect human rights. It has become widely accepted that businesses do have a corporate responsibility to respect human rights. The United Nations Guiding Principles on Business and Human Rights ('Guiding Principles') promote this responsibility as a global standard of expected conduct from business enterprises, regardless of their size, sector, operational context, ownership or structure.[1] Thus, from manufacturers to service-providing enterprises, all actors in the value chain are subject to the same responsibility.[2] In this sense, the corporate responsibility to respect human rights applies equally to enterprises

☆ This research is funded by the European Union's Horizon 2020 research and innovation programme under the Secure Collaborative Intelligent Industrial Automation (SeCoIIA) project, grant agreement No 871,967. The authors have contributed equally to this work. The authors would like to thank Dr Anil Yilmaz-Vastardis for her insightful comments on earlier drafts of this paper and suggestions for improvement and future research. As always, any errors or oversights are ours alone.

* Corresponding author.
E-mail address: ivo.emanuilov@kuleuven.be (I. Emanuilov).

[1] United Nations Human Rights Council, 'Guiding Principles on Business and Human Rights' (2011) A/HRC/17/31, Principles 11, 14.

[2] Importantly, the Guiding Principles refer to 'value chain', meaning the entire lifecycle of a product or service, which also includes business partners that are not necessarily suppliers. In this sense, the concept 'value chain' is broader than 'supply chain'. See also Lise Smit and others, *Study on Due Diligence Requirements through the Supply Chain: Final Report* (2020) 159–160. <https://op.europa.eu/publication/manifestation_identifier/PUB_DS0120017ENN> accessed 7 August 2020.

https://doi.org/10.1016/j.jrt.2022.100028
Received 13 November 2021; Received in revised form 11 February 2022; Accepted 17 February 2022
Available online 22 February 2022

engaged in traditional manufacturing as well as those in smart manufacturing driven by the developments in so-called Industry 4.0.

Let's illustrate this with some examples. In the near future, workers would be expected to interact increasingly with collaborative robots on the shop floor. Incidents and accidents caused or contributed to by such robots may have adverse impact on the right to life. The right to life might also be adversely impacted by cyber attacks on safety-critical industrial control systems. Increased workplace surveillance and discrimination in scenarios where humans and robots collaborate create tangible adverse impacts to the right to privacy or non-discrimination.[3] Similarly, procuring data or additive manufacturing services from companies or States where violations of these rights are known to take place on a large scale could have adverse impact on rights and freedoms, such as non-discrimination, freedom of expression, the right to life, the right to work etc. The possibilities for adverse human rights impacts, therefore, increase with the extension of manufacturing beyond the confines of a single factory's shop floor. The new models of manufacturing are associated with legally distinct and geographically spread manufacturers and service providers which pool common resources to form so-called 'smart factories' enabled by technological and organizational drivers, colloquially referred to as Industry 4.0.

This article offers a conceptual blueprint of challenges and perspectives on a new research sub-domain in the business and human rights scholarship that has not previously been studied, namely Industry 4.0 and human rights. The article is aimed at an interdisciplinary audience of corporate and human rights lawyers, legal and engineering professionals, business ethics experts and academics in law, ethics and engineering. It further aims to incentivize policymakers to consider both the human rights impacts and the opportunities for mitigation presented by Industry 4.0. We depart from the starting point of horizontal, vertical and end-to-end alignment of actors in collaborative manufacturing driven by smart technologies. We argue that this alignment could make discharging the corporate responsibility to respect human rights more challenging. In the Factories of the Future, novel approaches to and paradigms of manufacturing raise new issues. These issues include, broadly speaking, the horizontal diffusion of control in traditionally vertical manufacturing value chains, the difficulties in identifying responsible actors in data supply chains and (formal) verification of the provenance of digital raw materials, which are becoming essential in contemporary manufacturing practices, as well as the use of customer data in the production and maintenance of products and services. These challenges require a collaborative approach to human rights due diligence, as the main tool to discharge the responsibility of businesses to respect human rights. This article offers the idea of collaborative human rights due diligence as a decentralised approach that requires the joint action of actors operating on different levels in the supply chains to collaboratively identify and mitigate aggregate risks in their business models and operations.

We understand collaborative human rights due diligence as a collective, decentralised activity which entails both horizontal and vertical collaboration between actors on different planes and perhaps even in different industries (e.g., manufacturing, cloud computing, data analytics etc.). These actors would often be subject to different jurisdictions and sector-specific regulations. This article's main argument is that the pooling of due diligence efforts in a particular manufacturing industry, such as aerospace manufacturing, could have spill over effects of incentivising businesses in other industries to collaborate also on providing collective remedy.

The article is structured in four main parts. The first part traces back the origins of key concepts, such as Factories of the Future, to the notion of Industry 4.0. This part provides a brief introduction into the technologies underpinning Industry 4.0 and the overall impact of servitisation on manufacturing and the related human rights challenges. The second part introduces the concept of cyber-physical supply chains and its central role in Industry 4.0. The third part focuses on the corporate responsibility to respect human rights in the context of Industry 4.0. This part discusses the role of the *smart* manufacturer and the horizontal alignment of other supply chain actors in the Factories of the Future and the challenges to discharging their corporate responsibility to respect human rights. The fourth and final part presents a blueprint of a framework of how human rights due diligence could be conducted in collaborative smart manufacturing.

2. Industry 4.0, factories of the future and smart manufacturing: the human rights challenge of (Collaborative) smart manufacturing

As a preliminary remark, it should be highlighted that the concepts of Factories of the Future and Smart Manufacturing illustrate ideas that are still under development by the industry around the world. They are characterised by the deployment of various technologies aimed at full digitalisation of the manufacturing process and its transformation into an on-demand, customised service. The origins of these paradigms, however, lie in the broader notion of Industry 4.0, described in scholarship as a collective term for technologies and concepts of value chain organisation.[4]

2.1. Industry 4.0

Originally developed in the framework of the German industrial policy, the concept of Industry 4.0 refers to a set of technological changes in manufacturing whose main driver was the maintenance of continuing global competitiveness of the German industry.[5] In this context, Industry 4.0 is the organisation of production processes based on technologies and devices which communicate autonomously with each other along the value chain. In its broader sense today, Industry 4.0 is said to embrace "more broadly the technological, organizational, economical and societal changes driven by enhanced digitization of manufacturing industry".[6]

McFarlane highlights that Industry 4.0 is related to four main trends in manufacturing: specialisation, customisation, distribution and servitisation.[7] Specialisation implies that in the factories of the future manufacturers "need to be good at automating not just how they make things but how they set up the equipment to make things".[8] Furthermore, the increasing capability to track goods and assets along the supply chain

[3] Phoebe Moore, *Study on Data Subjects, Digital Surveillance, AI and the Future of Work* (European Parliament Research Service, 2020) 53, <https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf> accessed 12 October 2021.

[4] Jon Kepa Gerrikagoitia and others, 'Digital Manufacturing Platforms in the Industry 4.0 from Private and Public Perspectives' (2019) Multidisciplinary Digital Publishing Institute 14, 9 Applied Sciences 2934, 1. For a brief summary of the different emerging manufacturing paradigms, see Mohsen Moghaddam and others, 'Reference Architectures for Smart Manufacturing: A Critical Review' (2018) 49 Journal of Manufacturing Systems 215, 216.

[5] Jan Smit and others, 'Industry 4.0' (2016) Study IP/A/ITRE/2015-02 20 <https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf> accessed 12 March 2020.

[6] Adrien Bécue, Isabel Praça and João Gama, 'Artificial Intelligence, Cyber-Threats and Industry 4.0: Challenges and Opportunities' (2021) Artificial Intelligence Review 3 <10/gjxhdv> accessed 9 May 2021.

[7] Duncan McFarlane, 'Factories of the Future and Implications for Automation' (*University of Cambridge, Institute for Manufacturing Insights*) <https://www.ifm.eng.cam.ac.uk/insights/automation/factories-of-the-future-and-implications-for-automation/> accessed 11 March 2020.

[8] ibid.

creates room for customisation and the development of both novel quality control and accountability mechanisms.[9] The abilities created by automation to coordinate multiple production sites with just one system enables distribution of the manufacturing process. Finally, combining a physical product with a service that is usually subscription-based, and which adds new value to the physical product, is typical of the ongoing trend of servitisation of manufacturing.[10] The bundling of services with goods has been significantly facilitated by the digitalisation of factories and the emergence of new aftermarket services.[11]

These four trends are a function of the main features of Industry 4.0, namely interoperability, virtualisation, decentralisation and real-time decision-making, service orientation and modularity.[12] In Industry 4.0 these features are enabled, amongst others, by a distributed system of cyber-physical assets, also known as Internet of Things (IoT).

IoT involves three main types of components operating on different levels.[13] The first level is the so-called edge functionality. This is basically a set of sensors connected to physical objects and machines. For example, sensors could be deployed in a mining site where they monitor the sourcing of a particular mineral. The second level is that of data gateways, i.e., solutions for receiving and transmitting the data to and from the sensors.[14] In our mining example, data gateways may perform aggregation, pre-processing, optimisation etc. of data collected from the sensors. The third level is that of data management and analytics where data is collected, then linked, analysed and used, usually in a cloud environment, in order to generate insights and subsequent value. In our example, these may be insights about the characteristics of a mineral, progress of the mining operations, or even compliance with health and occupational safety requirements. These latter may be indicators, for example, as to whether the work schedule is respected, whether the occupational environment is safe enough etc.

In the manufacturing industry, Industrial IoT (IIoT) platforms integrate cyber-physical systems and data analytics services. These platforms are usually deployed for two main purposes: (1) collection of non-production data to improve industrial operations and (2) collection of product-related data to improve product lifecycle performance. Regardless of the purpose, they enable the manufacturer to get access to data originating from any third party along the supply chain.[15] It also allows real-time access to product and product-related data. In a traditional environment, these datasets would typically be stored in multiple and often incompatible with each other databases of suppliers, distributers, retailers, service providers etc.[16] In the context of Industry 4.0, however, the manufacturer would overcome these barriers and expand the value of their manufacturing infrastructure.

In a nutshell, Industry 4.0 is shaped by the introduction of ICT in the manufacturing processes. At its core, it is a collective term which refers to ICT and concepts for the organisation of value chains which have profound implications of how manufacturing is organised in the so-called 'smart factories', also known as Factories of the Future.[17]

2.2. The factory of the future (FoF)

FoF is a technical and organisational paradigm that builds on Industry 4.0. The systems in the FoF would be able to monitor and analyse physical processes by creating digital twins (i.e., virtual copies and simulations) of objects or environments from the physical world and enable decision-making based on self-organisation mechanisms.[18]

In the FoF, physical objects would be fully integrated into an information network which enables the vertical, horizontal and end-to-end integration of production systems. Vertical integration concerns intra-company integration and it is often pointed as the "foundation for exchanging information and collaboration amongst the different levels of the enterprise's hierarchy such as corporate planning, production, scheduling or management".[19] Indeed, it is vertical integration that digitises the enterprise by combining data from various manufacturing processes.[20] Horizontally, integration is manifested in the capability for real-time management of geographically spread value networks across different companies.[21] Therefore, horizontal integration is seen as "the foundation for a close and high-level collaboration between several companies, using information systems to enrich product lifecycle, creating an inter-connected ecosystem within the same value creation network".[22] Finally, end-to-end integration concerns the involvement of the customer side in the manufacturing process. End-to-end integration focuses on "closing gaps between product design and manufacturing and the customer, e.g., from the acquisition of raw material for the manufacturing system, product use and its end-of-life".[23]

These integration processes indicate that connected, or smart, factories are becoming elements of distributed production networks. This is a challenge to the paradigm of conventional manufacturing. In a smart factory, different elements of the same manufacturing process may take place in different geographical locations. The driving forces of digital transformation of the industry thus seem to do away with the classical verticality of traditional supply chains in favour of a more horizontal value chain.

This horizontal alignment involves not only suppliers and subcontractors but reaches further into the customer side. It also involves new stakeholders, such as cloud manufacturing service providers, data service providers and others. These new actors in the horizontal value chain play an important role. For example, they may operate a digital twin of the entire manufacturing environment which is capable of generating insights relevant to the physical production environment. This indicates a new shift towards collaborative smart manufacturing whereby all actors along the manufacturing value chain are involved to a certain degree in the manufacturing activity simultaneously.

This wide reach of collaboration hints that the activity itself extends

[9] The use of operational technology forensics need not be limited to investigation of security or safety incidents or accidents. Indeed, compliance artefacts produced by such processes could be used to the advantage of better application of business and human rights. This is particularly true for victims of adverse human rights impacts where much needed evidence is necessary for the effective implementation of their right to effective remedy.

[10] Tim S Baines and others, 'The Servitization of Manufacturing: A Review of Literature and Reflection on Future Challenges' (2009) 20 Journal of Manufacturing Technology Management 547, 547.

[11] Shin-yi Peng, 'A New Trade Regime for the Servitization of Manufacturing: Rethinking the Goods-Services Dichotomy' (2020) 54 Journal of World Trade 702–703 <http://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/54.5/TRAD2020030> accessed 17 November 2020.

[12] Smit and others (n 5) 21.

[13] Duncan McFarlane, 'Industrial Internet of Things: Applying IoT in the Industrial Context' (2018) 3 <https://www.ifm.eng.cam.ac.uk/uploads/DIAL/industrial-internet-of-things-report.pdf> accessed 11 March 2020.

[14] The European Commission foresees that the majority of data in the foreseeable future will originate from computing devices located at the edge of the network. See European Commission 'White Paper on Artificial Intelligence—A European approach to excellence and trust' COM(2020) 65 final, 19.02.2020, 1.

[15] McFarlane (n 13) 8.

[16] ibid.

[17] Gerrikagoitia and others (n 4) 1.

[18] Smit and others (n 5) 20. See also Gerrikagoitia and others (n 4) 1.

[19] Vítor Alcácer and Virgilio Cruz-Machado, 'Scanning the Industry 4.0: A Literature Review on Technologies for Manufacturing Systems' (2019) 22 Engineering Science and Technology, an International Journal 899, 911.

[20] ibid.

[21] Smit and others (n 5) 20.

[22] Alcácer and Cruz-Machado (n 19) 910.

[23] ibid 911.

beyond the realm of the physical factory and the temporal dimensions of manufacturing as a process with a clearly defined beginning and an end.[24] Indeed, the vertical integration and horizontal alignment of actors in the supply chain of collaborative smart manufacturing is better depicted as a network of continuously interacting actors rather than a static sequential chain of transactions between independent entities.

To sum up, the FoF is based on cyber-physical production systems which enable distribution of the manufacturing process across different geographical locations and decentralised decision-making. The FoF entails horizontal, vertical and end-to-end integration which allows the interconnection of factories located in different physical locations. By pooling their resources, manufacturers become a part of distributed production networks driven by novel manufacturing approaches such as smart manufacturing.[25]

2.3. Smart manufacturing

Smart manufacturing is a generic term and a new approach to manufacturing which aims to transform the traditional factories into the FoF. It refers to the deployment of ICT-based solutions across the manufacturing value chain.[26] The goal of smart manufacturing is not just to create more customised, diversified and mass-produced products, but also to enable flexible reaction to dynamic market changes.[27] Smart manufacturing depends on the full-scaled deployment of IIoT, resource virtualisation, cloud manufacturing, collaborative robots and artificial intelligence (AI).

Smart manufacturing is based on the paradigm of servitisation as it is driven by different, data-intensive processes, compared to traditional manufacturing. This means that manufacturing would no longer be limited to the process of converting extracted raw materials into a physical product.[28] Consequently, smart manufacturing has manifestations not only in cyberspace but also in the physical world. Thus, it depends on underlying operational technology and information technology infrastructure, such as sensors, cloud-based infrastructure, production facilities and assets, as well as their digital twins, which may be geographically spread across multiple States.

For example, a customer may place an order through a cloud manufacturing platform which offers a selection of suitable providers and supply chain contractors. They may have their product 3D printed in a location of their choice. Furthermore, data-driven customisation and personalisation provide customers with an opportunity to get products that are tailored to their specific needs.

This geographical distribution of factories and manufacturing assets leads to the emergence of cyber-physical supply chains overlaying the traditional manufacturing value chain. These assets and accompanying infrastructure are increasingly interconnected, automated and geographically distributed. This exposes supply chain actors to greater risk of non-compliance, amongst others, with internationally recognised human rights. Unlike physical assets, digital assets are non-rivalrous in that they may have multiple copies and be subject to concurrent processing in various locations under different jurisdictions. For example, datasets used for the training of machine learning models may originate from non-democratic regimes and their collection may be the result of violations of the right to privacy, non-discrimination,[29] or even the right to life. The same holds true of the deployment of machine learning models, e.g., to perform facial and speech/voice recognition or emotion detection, which are all considered essential in future manufacturing processes.

2.4. The human rights challenge of (collaborative) smart manufacturing

Cyber-physical supply chain actors, such as engineering contractors, cloud manufacturing service providers, data services providers etc., are becoming increasingly aware of their corporate responsibility to respect and provide remedy for human rights violations.[30] In the framework of the Guiding Principles, this responsibility is discharged primarily through the requirement to conduct human rights due diligence.[31] However, in the context of FoF driven by smart manufacturing approaches this may become more challenging for a number of reasons.

First is what Thompson defines as the problem of 'many hands'[32] and its corollary diffusion of control that makes it difficult to identify the responsible party. This problem is undoubtedly present also in traditional supply chains. However, certain design and operational features of cyber-physical supply chains, such as the ability to dynamically reorganise supply chains, resource virtualisation, and growing reliance on services of actors that are 'external' to the manufacturing process, make identifying the responsible party(ies) a much more challenging undertaking.

Second, the geographical distribution of cyber and physical assets complicates the process of *ex ante* human rights due diligence. In traditional supply chains, a manufacturer has clearly established business relationships, usually structured by means of long-term contractual agreements. Therefore, there is a certain measure of **theoretical** *ex ante* predictability as to what is to be expected from a particular business relationship. However, in settings which extend beyond the physical boundaries of one or more factories operated by the same manufacturer, a manufacturer may no longer know the exact provider of a particular resource provided or service rendered. Furthermore, it is possible that a digital asset is ultimately the result of multiple data transactions and processing operations that are not always easy to trace.

Third, the architecture of human rights due diligence in the Guiding Principles is premised on individual actors being ultimately responsible for carrying out due diligence of their value chains and business

[24] Orian Dheu, Charlotte Ducuing and Peggy Valcke, 'The Emperor's New Clothes: A Roadmap for Conceptualizing the New Vehicle' (2020) TRANSIDIT 12, 14–15.

[25] Sameer Mittal and others, 'Smart Manufacturing: Characteristics, Technologies and Enabling Factors' (2019) 233 Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture 1342, 1342.

[26] In its program on Smart Manufacturing Operations Planning and Control, the US National Institute of Standards and Technology (NIST) refers to 'smart manufacturing' as to "fully-integrated, collaborative manufacturing systems that respond in real time to meet changing demands and conditions in the factory, in the supply network, and in customer needs", National Institute of Standard and Technology, 'Smart Manufacturing Operations Planning and Control' (2014) <https://www.nist.gov/system/files/documents/2017/05/09/FY2014_SMOPAC_ProgramPlan.pdf> accessed 17 November 2020.

[27] European Commission, 'Smart Manufacturing' (*Shaping Europe's digital future - European Commission*, 8 August 2018) <https://ec.europa.eu/digital-single-market/en/smart-manufacturing> accessed 23 March 2020.

[28] Mittal and others (n 25) 1342.

[29] Brett Aho and Roberta Duffield, 'Beyond Surveillance Capitalism: Privacy, Regulation and Big Data in Europe and China' (2020) 49 Economy and Society 187, 194.

[30] Admittedly, however, the technology sector has a very limited view of its stakeholders and this may prove problematic when it comes to addressing actual or potential adverse human rights impacts. See Robert McCorquodale and others, 'Human Rights Due Diligence in Law and Practice: Good Practices and Challenges for Business Enterprises' (2017) 2 Business and Human Rights Journal 195, 210.

[31] United Nations Human Rights Council (n 1), Principle 17.

[32] Dennis F Thompson, 'Responsibility for Failures of Government: The Problem of Many Hands' (2014) 44 The American Review of Public Administration 259, 259. See also A Nollkaemper, 'The Problem of Many Hands in International Law' (2015) Amsterdam Law School Legal Studies Research Paper <https://dare.uva.nl/search?sort=year;field1=dai;value1=075187744;docsPerPage=1;startDoc=32> accessed 7 February 2020.

relationships.[33] However, this approach does not translate well to multi-actor environments where distributed industrial assets may automatically perform delegated tasks and where we have predictive and optimisation tasks throughout the lifecycle of these assets. For example, a military aircraft system's digital twin, which incorporates predictive analytics, may inform an optimisation decision to use operational data from a battlefield operation in an armed conflict. On one hand, this could have significant legal ramifications for the manufacturer, but, on the other, it may as well remain unnoticed.[34]

Fourth, collaborative smart manufacturing implies the horizontal integration of different actors in both the industrial and the data value chain. This suggests not only integration of assets through digital connectivity on the production floor and across manufacturing facilities, but also integration of third-party suppliers and service providers within the supply chain through automated operations and collaboration. As no single actor has a complete view of the cyber-physical interactions between machines and humans, it is unclear who can or should supervise these activities to ensure compliance with human rights law and to mitigate the aggregate risks along the supply chain.

Finally, effective human rights due diligence rests on an end-to-end view of the supply chain. In cyber-physical supply chains, operational technology[35] forensics could help to discover evidence crucial for risk mitigation. However, the forensics techniques currently available do not operate well in collaborative smart manufacturing environments. In these environments commercially sensitive information and operational technology devices are spread across many artefacts, such as field devices, collaborative robots etc. Conversely, these devices may be under the control of actors spread across multiple geographical locations and jurisdictions which may significantly hinder access to remedy.[36]

These specific human rights challenges in smart manufacturing indicate the clear necessity for a comprehensive human rights due diligence (HRDD) in Industry 4.0 that would need to incorporate some unique elements and methodology which would allow it to fully serve its purpose. The following sections of the article are going to explore the issues that a traditional HRDD would face in the context of smart manufacturing and a proposed solution to them.

3. Responsibility to respect human rights in industry 4.0: human rights due diligence in collaborative smart manufacturing

The corporate responsibility to respect human rights is central to the idea of responsible business conduct. Indeed, one of the foundational principles of this second pillar of the Guiding Principles is that business enterprises should respect human rights. This means enterprises should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved.[37]

The material scope of this responsibility is broad.[38] On the one hand, business enterprises should avoid causing or contributing to adverse human rights impacts through their own activities. On the other hand, they should also seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships; that is, even if they have not contributed to these impacts.[39] Smart manufacturing and the related pluralisation of this responsibility makes it much harder to determine who or what causes, contributes to or is linked with a particular harm. This also has implications for how companies discharge their corporate responsibility to respect through human rights due diligence.

3.1. Concept of human rights due diligence

Central to the corporate responsibility to respect human rights is the process of human rights due diligence. In order to discharge this responsibility, business enterprises must conduct human rights due diligence.[40] As the UN Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, Prof. John Ruggie, pointed out, due diligence indicates the "steps a company must take to become aware of, prevent and address adverse human rights impacts".[41]

Scholars, such as Mazzeschi and Cassella, have shown that the concept of due diligence is multifaceted and is often the source of profound disagreement amongst legal scholars.[42] For example, in public international law, due diligence may be seen as characterising a particular set of international obligations, as a principle of international law, or indeed as an independent general rule of international law.[43] These opinions are particularly justifiable looking at private law, where due diligence most often refers to a particular standard of care in discharging an obligation.[44] Conversely, due diligence has a particular meaning in a corporate context as a business management practice dealing with and mitigating risks to the business enterprise. Thus, unlike human rights due diligence, enterprise risk management looks at enterprise-related risks, which are often company-specific, and aims to prevent risks mainly to employees or the business itself.[45] Finally, in a business and human rights context, due diligence has specific meaning as a management process to mitigate human rights impacts. These impacts may be caused or contributed to *by* a business enterprise or directly linked *to* its operations, products or services through its business relationships.[46]

[33] James Harrison, 'Establishing a Meaningful Human Rights Due Diligence Process for Corporations: Learning from Experience of Human Rights Impact Assessment' (2013) 31 Impact Assessment and Project Appraisal 107, 107.

[34] Alexander Kott, 'Intelligent Autonomous Agents Are Key to Cyber Defense of the Future Army Networks' (2019) The Cyber Defense Review 57, 65.

[35] Operational technology is defined as hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes and events. See Gartner, 'Operational Technology (OT)' (*Gartner Glossary*) < https://www.gartner.com/en/information-technology/glossary/operational-technology-ot> accessed 24 March 2020.

[36] Jennifer A Zerk, 'Extraterritorial Jurisdiction: Lessons for the Business and Human Rights Sphere from Six Regulatory Areas' (2010) Working Paper No. 59 5 <https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/workingpaper_59_zerk.pdf> accessed 2 April 2021.

[37] United Nations Human Rights Council (n 1), Principle 11, 13.

[38] Claire Methven O'Brien and Sumithra Dhanarajan, 'The Corporate Responsibility to Respect Human Rights: A Status Review' (2016) 29 Accounting, Auditing & Accountability Journal 542, 545.

[39] United Nations Human Rights Council (n 1), Principle 13.

[40] ibid Principle 15 (b).

[41] United Nations Human Rights Council, 'Protect, Respect and Remedy: a Framework for Business and Human Rights: Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie' (2008) A/HRC/8/5, para 56.

[42] Ricardo Pisillo Mazzeschi, 'Le chemin étrange de la due diligence: d'un concept mystérieux à un concept surévalué' in Sarah Cassella (ed), *Le standard de due diligence et la responsabilité internationale: Journée d'études franco-italienne du Mans* (Éditions A Pedone 2018) 324–325.

[43] ibid 323–325.

[44] Smit and others (n 5) 158.

[45] See an overview of the differences between human rights due diligence and business management in McCorquodale and others (n 30) 199–201. For more information on the differences and similarities between enterprise risk management and human rights due diligence, see B Fasterling, 'Human Rights Due Diligence as Risk Management: Social Risk versus Human Rights Risk' (2017) 2 Business and Human Rights Journal 225, 227–230.

[46] Some critics have described this latter meaning of due diligence as a concept with more of a political rather than legal value. See Pisillo Mazzeschi (n 42) 325.

In the context of business and human rights, there is an intrinsic nexus between the State duty to protect and the corporate responsibility to respect human rights. Indeed, as noted by the UN Committee on Economic, Social and Cultural Rights, the State obligation to protect human rights entails a positive duty to adopt laws requiring businesses to exercise human rights due diligence.[47] This requires States to mandate that corporations deploy their best efforts to make sure that entities whose conduct these businesses may influence respect international human rights.[48]

The Guiding Principles do not define human rights due diligence explicitly. In its interpretative guide, the Office of the High Commissioner for Human Rights has suggested that due diligence is an "ongoing *management process* that a reasonable and prudent enterprise needs to undertake, in the light of its circumstances (including sector, operating context, size and similar factors) to meet its responsibility to respect human rights" (emphasis added).[49] The purpose of human rights due diligence is therefore to identify, prevent, mitigate and account for how business enterprises address their adverse human rights impacts.[50] The process entails the identification and assessment of both actual and potential human rights impacts.[51] Business enterprises are then required to integrate and act upon their findings, to track responses and to communicate how the impacts are being addressed. Human rights due diligence is an ongoing process which recognises that these impacts may change over time as the business enterprise's operations evolve.[52] It further acknowledges that the risks may vary depending on size of the enterprise and the nature and context of its operations.[53]

There has been much scholarly debate on the concept of human rights due diligence and its nature and content. One such notorious example is the exchange between Bonnitcha and McCorquodale, on one side, and Ruggie and Sherman, on the other, arguing about the allegedly purely legal (or not) nature and scope of HRDD.[54] While this debate is beyond the scope of this article, we subscribe to the view that for businesses the Guiding Principles indeed aim to go beyond mere legal compliance by "focus[ing] on the need to manage the risk of involvement in human rights abuses, which requires that companies act with due diligence to avoid infringing on the rights of others and address harm where it does occur".[55] Human rights due diligence can therefore be seen rightly as a mechanism for acquiring knowledge about human rights violations.[56]

3.2. Challenges to human rights due diligence in collaborative smart manufacturing

As already pointed out, the corporate responsibility to respect is applicable to all kinds of business enterprises, regardless of the sector, type, size, nature or context of operations. Therefore, conducting human rights due diligence is required equally from all enterprises, regardless of their position in the value chain, i.e. whether they are manufacturers, suppliers, supply chain or engineering contractors, or service providers. In the context of collaborative smart manufacturing, and more generally in Industry 4.0, however, there appear to be a number of challenges which may not be sufficiently covered by the processes used to discharge the corporate responsibility to respect, as enshrined in the Guiding Principles.

3.2.1. The position of the manufacturer

The first main challenge is related to the problem of control diffusion at the level of the manufacturer, the supply chain actors and the customer. Indeed, in cyber-physical supply chains, the manufacturer may assume two somewhat conflicting roles.

The first possible role of a manufacturer is that of the organising and orchestrating entity. Equipped with a network of sensors deployed at materials sourcing sites (e.g., a mining facility), industrial systems, collaborative robots and data analytics services, the manufacturer's economic and legal power clearly increases.[57] In an ideal scenario, the manufacturer could thus be seen as an omnipotent entity that has a full and dynamic oversight of the activities of its suppliers, (sub-)contractors, service providers and data flows.

Unlike traditional manufacturing, analytical services in collaborative smart manufacturing would provide the manufacturer with a rich, dynamic and real-time picture of the relationships and dependencies in the supply chain. In this sense, its capacity to conduct human rights due diligence and to identify and prevent human rights impacts could be significantly higher than that of a traditional manufacturer. For example, the availability of predictive and preventive machine learning models could be used to gain insights into and predict where and when a particular business process could fail or underperform. Equally, such insights could be used to proactively manage risks of adverse human rights impacts, for instance concerning a failure of or defect in a collaborative robot that might endanger workers' health and safety.[58]

Commentators have rightly pointed out that although human rights due diligence in the context of business and human rights is seen as a management standard, it can nevertheless also inform the content of a due diligence liability standard.[59] Therefore, the manufacturer's enhanced capability to exercise control and supervision over the potential sources of human rights impacts may also entail a higher standard of due diligence in the law of negligence.

The second possible role of a manufacturer is that of a 'first amongst equals'. In this case the manufacturer is seen not as an organising entity, but rather as a node in a complex cyber-physical supply chain.

For example, in the context of smart manufacturing, the manufacturer could have the physical aeroplane being assembled on the shop

[47] United Nations Economic and Social Council, Committee on Economic, Social and Cultural Rights, 'General Comment No. 24 (2017) on State obligations under the International Covenant on Economic, Social and Cultural Rights in the context of business activities' (2017) E/C.12/GC/24, para 16.

[48] ibid 33.

[49] Office of the UN High Commissioner for Human Rights, 'The Corporate Responsibility to Respect Human Rights: An Interpretive Guide' (2012) HR/PUB/12/02 6 <https://www.ohchr.org/Documents/publications/hr.puB.12.2_en.pdf> accessed 24 March 2020.

[50] United Nations Human Rights Council (n 1), Principle 17.

[51] James Harrison, 'Human Rights Measurement: Reflections on the Current Practice and Future Potential of Human Rights Impact Assessment' (2011) 3 Journal of Human Rights Practice 162, 166.

[52] United Nations Human Rights Council (n 1), Principle 17 (c).

[53] ibid Principle 17 (b).

[54] Jonathan Bonnitcha and Robert McCorquodale, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights' (2017) 28 European Journal of International Law 899; John Gerard Ruggie and John F Sherman, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights: A Reply to Jonathan Bonnitcha and Robert McCorquodale' (2017) 28 European Journal of International Law 921; Jonathan Bonnitcha and Robert McCorquodale, 'The Concept of "Due Diligence" in the UN Guiding Principles on Business and Human Rights: A Rejoinder to John Gerard Ruggie and John F. Sherman, III' (2017) 28 European Journal of International Law 929.

[55] John Gerard Ruggie, 'Global Governance and "New Governance Theory": Lessons from Business and Human Rights' (2014) 20 Global Governance: A Review of Multilateralism and International Organizations 5, 9.

[56] Fasterling (n 45) 228.

[57] On the distinction and relationship between power and authority of multinational enterprises, see John Gerard Ruggie, 'Multinationals as Global Institution: Power, Authority and Relative Autonomy: Multinationals as Global Institution' (2018) 12 Regulation & Governance 317, 11.

[58] David Cabrelli and Richard Graveling, 'Health and Safety in the Workplace of the Future' (2019) Briefing PE 638.434 3–4 <https://op.europa.eu/en/publication-detail/-/publication/e2f19fe1-e32d-11e9-9c4e-01aa75ed71a1/language-en> accessed 14 October 2021.

[59] Fasterling (n 45) 228.

floor. At the same time, a cloud manufacturer could have access to a real time digital copy (i.e., a digital twin) of the aeroplane, on which various participants in the value chain could collaborate simultaneously. To make things even more complicated, the digital copy could be updated and improved with feedback data from airplanes that are already in exploitation. This 'dispersed' manufacturing process would effectively transform the manufacturer into just another link in the chain, blurring the notion of control.

These two conflicting roles of the manufacturer do not depend on its status as a legal subject but are instead determined by the nature of collaborative smart manufacturing. Against this background, human rights due diligence is premised on the idea that it is within the business enterprise's control to prevent or mitigate human rights impacts at the beginning of a new business relationship or activity.[60] Indeed, an enterprise may structure its relationships using agreements that mandate a degree of due diligence from its contractual partners in the discharge of their obligations. However, this may not be as straightforward when it comes to processes within Industry 4.0 which may be based on data-driven, autonomous decision-making.

Kriebitz and Lütge identify four situations where using data-driven autonomous decision-making might entail human rights violations: (1) input data conflicting with human rights; (2) output leading to unintended human rights violations; (3) use in specific areas conflicts with human rights; and (4) use of data-driven technologies by human rights violators.[61]

All four scenarios could apply in the context of collaborative smart manufacturing. In particular, the input data and the potential customer's use of a 'smart' product to violate human rights raise two main concerns of control over operations, products and services.

The first scenario is related to a manufacturer's control over the digital 'raw' materials supplying data-driven autonomous decision-making and production processes. Many of these digital 'raw' materials would consist of data sets and data-derived products or services involving the processing of both personal and commercially sensitive non-personal data. In these cases, data provenance, i.e., the ability to trace the history of derivation of a data artefact from its sources,[62] would be essential to ensuring that their use is not related with or contributing to adverse human rights impacts. From a human rights law perspective, this entails compliance not only with the basic principles of data protection law (e.g., in EU law these are lawfulness, fairness and transparency, purpose limitation, data minimization, storage limitation, accuracy, integrity and confidentiality and accountability), but also with the right to privacy and the right to property, in cases and jurisdictions where property rights or other exclusive rights over data may be recognized.

The second scenario refers to the extent of control that a manufacturer may have over the potential customer's use of data-driven products. These can be cases where the customer uses a connected product that feeds data of how it is used back to the manufacturer. For example, if the customer engages in malicious practices, e.g., deployment of facial recognition technology for secure verification of customers of an application or service that is used also for surveillance or profiling of minorities or other vulnerable groups, the manufacturer could find itself in possession of data that indicate such malicious practices with a high degree of probability. Furthermore, depending on the contractual relationship with the customer, the manufacturer may have full, limited or minimal access to such data, and they may or may not be allowed to process such data to derive further insights into the use case(s) of the customer. The question of whether the manufacturer's responsibility to respect human rights extends to such scenarios or not shows the limitations of human rights due diligence performed from the perspective of a single company to distributed data-driven processes within Industry 4.0.

The scenario where the output leads to adverse human rights impact is relatively well understood and is also related to the previous scenario. Through the lens of the customer, the usage of, for example, facial recognition technology in a way that causes adverse human rights impacts would clearly amount to failure on their part to discharge their responsibility to respect human rights. In this case, the responsibility is more clearly channelled solely through the customer since their choice of using certain technology for malicious purposes is independent of the manufacturer's control over the product. Still, it is interesting to hypothesize whether this would be the case also where the manufacturer could in fact put in place restrictive measures or limit the access to or functionality of a product or service upon becoming aware of uses that lead to adverse impacts on human rights.

Finally, the scenario where use in specific areas conflicts with human rights is just an instantiation of the principle that the characteristics of the operating context and the likelihood and severity of significant risks to human rights are crucial to determine whether human rights due diligence is appropriate. In this case smart manufacturing, particularly in industries that are inherently related with greater likelihood of adverse human rights impacts, such as defence and security, is just one example of a specific area which may conflict with human rights.

3.2.2. *The position of the supplier*

Suppliers in the smart manufacturing value chain could be two main types: suppliers of physical materials, incl. raw materials, and suppliers of digital materials, incl. digital raw materials. As previously mentioned, servitisation entails a shift in the traditional paradigm of the manufacturer in the driver's seat, configuring its business relationships with downstream suppliers of raw materials and services. Collaborative smart manufacturing entails new responsibilities for suppliers, such as maintaining adequate levels of cybersecurity and ensuring data provenance and lineage in their business operations.

In terms of cybersecurity, recent developments hint that supply chain security is now high on the agenda. For example, the proposal for a revision of the Network and Information Security Directive (NIS2) now includes provisions concerning supply chain security.[63] These provisions came after the Commission recognized the cybersecurity risks stemming from an entity's supply chain and the relationship with its suppliers. It was also recognized that there is an increasing number of instances when malicious actors were able to "compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third party products and services."[64] Therefore the NIS2 Directive requires entities to include into their risk assessment and take into account "the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures."[65] Moreover, the Cooperation group involving relevant national authorities, in cooperation with the Commission and ENISA is expected to carry on 'coordinated sectoral supply chain risk assessments'[66] following the already established practice for 5 G

[60] United Nations Human Rights Council (n 1), Principle 17.

[61] Alexander Kriebitz and Christoph Lütge, 'Artificial Intelligence and Human Rights: A Business Ethical Assessment' (2020) Business and Human Rights Journal 1, 12.

[62] Szymon Klarman, Stefan Schlobach and Luciano Serafini, 'Formal Verification of Data Provenance Records' (2012) The Semantic Web – ISWC 2012, Lecture Notes in Computer Science, 215–30, 215.

[63] European Commission, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 [2020] COM/2020/823 final, Article 18,2(d).

[64] European Commission (n 63), Recital 43.

[65] ibid, emphasis added.

[66] ibid, Recital 46 in conjunction with Article 19.

networks.[67] The overall goal here is to "address key supply chain risks and assist entities operating in sectors covered by the Directive to appropriately manage supply chain and supplier related cybersecurity risks."[68] What is important, however, is that sectorial supply chain risk assessment under NIS2 should take into account both technical and, where relevant, non-technical factors, including those defined in Recommendation (EU) 2019/534, in the EU wide coordinated risk assessment of 5 G networks security and in the EU Toolbox on 5 G cybersecurity agreed by the Cooperation Group.[69] The Directive also recommends a set of criteria to be taken into consideration when identifying which supply chains should be subject to coordinated risk assessment. These criteria are:

- the extent to which essential and important entities use and rely on specific critical ICT services, systems or products;
- the relevance of specific critical ICT services, systems or products for performing critical or sensitive functions, including the processing of personal data;
- the availability of alternative ICT services, systems or products;
- the resilience of the overall supply chain of ICT services, systems or products against disruptive events;
- the potential future significance for the entities' activities in the case of emerging ICT services, systems or products.

In light of these requirements, suppliers should now be transparent towards their customers not only about the features and properties of a particular material or service, but also about their cybersecurity practices and secure procurement and development procedures. It is expected to see such requirements maturing in contractual negotiations with suppliers. Furthermore, compliance with certain industry recognized standards or good practices could become an important criterion in human rights due diligence exercises. That is to say, failure to adopt secure procurement and development practices could be seen as creating a risk for adverse human rights impacts, e.g., concerning the confidentiality, integrity or availability of data and their relationship with certain human rights, such as the right to privacy.

In terms of data provenance and lineage, suppliers similarly will have to maintain an inventory of their data sources, keep records of their processing activities and ensure that any products and services derived from the processing of such data comply with the legal requirements applicable to the particular category of data. Thus, suppliers will have to consider not only the origin and transformations of the data during its lifecycle, but also the potential for adverse human rights impacts of products and services that are built on the basis of such data. For example, if a supplier uses a base pre-trained machine learning model for image recognition in a process known as transfer learning, they would have to scrutinize both the base pre-trained model and the retrained model. The use of pre-trained models is becoming commonplace due to their significantly smaller computational costs and the relatively lower requirements in terms of access to large datasets. However, transfer learning usually produces best results when the pre-trained model has been trained on large and reliable datasets where bias mitigation measures have been applied. This implies that the supplier should be in possession not only contractual but also technical warranties as to the quality attributes of the pre-trained model and this includes extending their human rights due diligence processes to any materials that serve as input for their products and services, including customer data that may be shared between manufacturer and supplier.

3.2.3. The position of the customer

The extent of control that a manufacturer may have over the potential customer's use of data-driven products is a major concern which indicates the new position of the customer in the manufacturing value chain. In 'servitised' collaborative smart manufacturing the product would no longer be a static object which, once it has left the shop floor, is outside the reach of the manufacturer. To the contrary, with the horizontal alignment of actors in the supply chain, the manufacturing process would reach further down the customer side.

On one hand, this may facilitate the customisation of a product to the customer's specific needs. On the other, it may create a feedback loop from the customer side all the way back to the manufacturer and other actors in the supply chain. This feedback loop may transmit back operational data which are used to maintain, optimise and improve the product. Such data transactions could have particular implications for the human rights due diligence of the manufacturer in some cases. For example, there may be one direct and one indirect customer, such as a company exporting certain products that may contain software that could be used for surveillance purposes to a State(s) which then commit violations of human rights.[70] Clearly, the State(s) and the manufacturer do not have a direct business relationship. Yet, an operational feedback loop created from the product back to the supply chain of which the manufacturer is part may create an indirect relationship between a violating State and a manufacturer. Ultimately, this brings in question the stability of the criterion of 'direct link'[71] between a human rights impact and a product om the context of smart manufacturing.

This example shows that the transition of manufacturing from streamlined coordination to diffuse collaboration in Industry 4.0 exhibit some difficulties which the process of human rights due diligence may encounter. This process assumes that a business undertaking is capable of structuring its business relationships in such a way as to enable it to carry out a systematic monitoring and mitigation of adverse human rights impacts.[72] Undoubtedly, this assumption is valid in the context of linear business operations which rely on structured and oftentimes hierarchical relationships between the actors in traditional supply chains.

3.2.4. The role of the digital raw materials

In addition to the evolution of the roles of the manufacturer and the customer in Industry 4.0, there is also an evolution in the understanding of the notion of raw materials. In recent years, we have seen noticeable rise of what can be described as digital raw materials that fuel smart manufacturing.[73] In this article, by the concept of 'digital raw materials' we refer mainly to datasets, machine learning models, digital twins and machine-generated artifacts which may be used in the manufacturing process. These 'raw' materials may originate from multiple and diverse sources and may often be subject to modifications along the supply chain.

At the level of procuring digital raw materials, the question is whether a manufacturer could trace the source of all datasets which may have served as input for the training or testing of a machine learning

[67] Commission Recommendation (EU) 2019/534 of 26 March 2019 Cybersecurity of 5 G networks [2019] OJ L88.
[68] European Commission (n 63), Recital 46.
[69] European Commission (n 63), Recital 47.

[70] This particular example is inspired by the *Amesys* case and its related civil and criminal judicial actions, as well as Recital 2, 5 of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) [2021] OJ L 206. See International Federation for Human Rights, Amesys Case: The Investigation Chamber green lights the investigative proceedings on the sale of surveillance equipment by Amesys to the Khadafi regime, 17 January 2013, available at: <https://www.refworld.org/docid/511cb668a.html>, accessed 28 February 2022.
[71] United Nations Human Rights Council (n 1), Principle 17.
[72] Olivier De Schutter and others, 'Human Rights Due Diligence: The Role of States' (2012) 50.
[73] Werner Struth, 'Data Is Key Raw Material for Industry 4.0' (*Bosch ConnectedWorld Blog*, 10 June 2015) <https://blog.bosch-si.com/industry40/data-key-raw-material-for-industry-40/> accessed 2 April 2021.

model which lies at the heart of their product. Several existing solutions from the practice of software engineering and data science could be adopted to address this problem. One solution for the software side is the so-called software bill of materials[74] which is, essentially, a list of ingredients of a software package, incl. supplier name, identifier, version string, component hash, relationship to other components, known vulnerabilities etc. A step further would be to engage in the creation of digital bill of materials which goes beyond the software side to include also interaction between components and a system's overall behavioural context.[75] On the data side, solutions such as datasheets for datasets could be adopted by manufacturers to keep a record of their own datasets and to demand from their suppliers the creation of datasheets which document the composition, intended uses, maintenance, and other relevant properties of datasets.[76] Together, software or digital bills of materials and datasheets for datasets could serve the objectives of human rights due diligence as far as the supply chain of digital raw materials is concerned.

The following example illustrates some of the difficulties manufacturers might face. For example, a manufacturer of unmanned aircraft systems may procure datasets from a company which is known for the high precision of its facial recognition software. Unbeknownst to the manufacturer, this latter company may have built the machine learning models for its application using data from, e.g., a conflict area or a detention camp.[77] These data may furthermore originate from multiple and diverse sources which makes it practically impossible for any single actor to detect potential risks. Indeed, similar concerns have been raised in the context of conflict minerals. Scholars have recognised that downstream companies are almost incapable to detect risks, the problem being not so much their unwillingness to comply, rather the complexity of managing the supply chain.[78] The same holds true of managing complex data supply chains, especially when datasets may be originating from conflict or high risk areas where there may be systemic violations of international humanitarian law and human rights law.

In such a complicated environment, it becomes very difficult for manufacturers to detect, prevent and mitigate adverse human rights impacts.

The logical distribution of processing operations also raises the question of whether physical access and control should be the main criteria to determine who has legal control over the data. Exercising physical control over data is not sufficient for such a finding. In the digital realm, logical control, e.g., remote access to cloud data, has been suggested as more practicable, for example, to exert jurisdiction over persons who control access to intelligible data and other digital raw materials, regardless of their location or means used to exercise such control, e.g., legal, organisational, or technical.[79] Such a finding can have profound implications on the due diligence obligations of manufacturers established in jurisdictions which have adopted laws mandating human rights due diligence.

In a nutshell, collaborative smart manufacturing in Industry 4.0 presents new challenges of technical, legal and organisational nature. We have tried to demonstrate that these challenges question the suitability of human rights due diligence conducted at the level of a single business enterprise to identify, prevent and mitigate adverse human rights impacts in complex cyber-physical supply chains. The final section of this article suggests a hybrid framework of collaborative human rights due diligence for Industry 4.0.

4. Adaptation of human rights due diligence for industry 4.0

After discussing the challenges faced by traditional human rights due diligence, when applied to the process of smart manufacturing, we would like to propose certain adaptations that, in our opinion, may mitigate some of the issues and generally prepare the industry to transition to smart manufacturing in a way that is compliant with the obligation to respect human rights.

It has long been established that the content and scope of human rights due diligence is determined by the context in which a company is operating, its activities, and its business relationships.[80] Indeed, the Special Representative hinted in his report that "[*a*]s companies adopt and refine due diligence practices, industry and multi-stakeholder initiatives can promote sharing of information, improvement of tools, and standardization of metrics".[81] The Guiding Principles, however, do not specify any modalities of a collaborative approach to human rights due diligence. The default position therefore remains that it is up to each company individually to discharge its corporate responsibility to respect human rights by conducting its own due diligence process. For the reasons stated in the preceding sections, the collaborative nature of manufacturing in Industry 4.0 presents specific challenges which can only be met by an equally collaborative process of human rights due diligence.

By collaborative human rights due diligence, this article understands a decentralised and joint action of actors operating on different tiers in a supply chain to collaboratively identify, prevent and mitigate (aggregate) risks in their business models and operations. Collaborative human rights due diligence is thus a collective decentralised activity which can also involve participants from different industries, often subject to different jurisdictions. The joint action of actors is the key element in this definition. The example of using pre-trained models in the previous section illustrated this need. The use of pre-trained models as the basis of new applications and services entails reliance on models that are computationally and financially expensive to replicate.[82] This also means that no individual supplier or manufacturer could independently fix errors or unexpected behaviour in their application or service resulting from a bug in the pretrained model. Even more importantly, any bug in the pre-trained model could be propagated into any product or service that relies on this model. The model's unexpected behaviour could be the result of choices made during the data collection and curation phase, or indeed in the training process itself. Perhaps not even the producer of the pretrained models would be able to independently

[74] Robert Alan Martin, 'Visibility & Control: Addressing Supply Chain Challenges to Trustworthy Software-Enabled Things' [2020] 2020 IEEE Systems Security Symposium (SSS) <10/gjmztw>.

[75] Dmitry Raidman, 'Why We Need a Software Bill of Materials Industry Standard' (*DevOps.com*, 20 August 2020) <https://devops.com/why-we-need-a-software-bill-of-materials-industry-standard/> accessed 2 April 2021.

[76] Timnit Gebru and others, 'Datasheets for Datasets' [2020] arXiv: 1803.09010 [cs] 1 <http://arxiv.org/abs/1803.09010> accessed 2 April 2021.

[77] Such as, for example, AnyVision's facial recognition software used by the Israeli military forces to carry out surveillance in the Occupied Palestinian Territories.

[78] Hannes Hofmann, Martin C Schleper and Constantin Blome, 'Conflict Minerals and Supply Chain Due Diligence: An Exploratory Study of Multi-Tier Supply Chains' (2018) 147 Journal of Business Ethics 115, 116. See also Miho Taka, 'Emerging Practice in Responsible Supply Chain Management: Closed-Pipe Supply Chain of Conflict-Free Minerals from the Democratic Republic of Congo' (2016) 121 Business and Society Review 37, 48.

[79] W Hon, *Data Localization Laws and Policy* (Edward Elgar Publishing 2017) 321 <https://www.elgaronline.com/view/9781786431967.xml> accessed 25 February 2020.

[80] United Nations Human Rights Council (n 41) para 25.

[81] ibid 64.

[82] Different sources provide different estimates, but it is believed that the cost of training GPT-3 varies between $4.6 million and $12 million USD. See Chuan Li, *OpenAI's GPT-3 Language Model: A Technical Overview*, Lambda Labs, June 03, 2020, available at: <https://lambdalabs.com/blog/demystifying-gpt-3/> accessed 28 February 2022, and Kyle Wyggers, *OpenAI launches an API to commercialize its research*, Venture Beat, June 11, 2020, available at: <https://venturebeat.com/2020/06/11/openai-launches-an-api-to-commercialize-its-research/> accessed 28 February 2022.

identify and resolve the issue, without coordinating its action with its own suppliers and contractors.

The veil of secrecy around machine learning-based products and services impedes transparency and accountability, which are key elements of the corporate responsibility to respect human rights. Transparency in the human-readable sources (e.g., training data sets, training scripts, environment simulators etc.) is a prerequisite for transparency of the machine learning process or product itself. We believe that one way to improve transparency is by open sourcing some of the building blocks of machine learning. Community-based peer review of open source machine learning products and services can not only improve human rights due diligence but can also help companies to build better, fairer and more transparent products and services that respect human rights. Furthermore, against growing calls for a more collaborative and open machine learning development,[83] any collaboratively developed models will likely depend on both community engagement and commercial support to remain sustainable and this unavoidably entails resource pooling and joint action, much like what we have seen in the field of open source software.[84] Ultimately, the main benefit of pooling human rights due diligence efforts in a particular manufacturing industry, e.g. aerospace manufacturing, is that it could produce network effects incentivising businesses to collaborate also on providing collective remedy.[85]

The proposed framework of collaborative human rights due diligence integrates elements from the three pillars of the Guiding Principles. Thus, the due diligence obligations of States refer to the first pillar, whereas supply chain due diligence and sectoral collaborative due diligence concern the second one. Finally, human rights-based standardisation refers to both human rights due diligence and access to effective remedy, as human rights-based considerations embedded in standards should contribute to products and services complying with such standards to also facilitate access to remedy Fig. 1.

In methodological terms, this framework is the result of research conducted with industrial large-scale companies and SMEs in the framework of the EU-funded research project Secure Collaborative Intelligent Industrial Assets (SeCoIIA).[86] Its findings are complemented by feedback collected during a workshop organized in May 2021 in the framework of this project.[87] The framework has been discussed with stakeholders from the manufacturing and cybersecurity industries, partnering organizations in the SeCoIIA project, as well as peers with an interdisciplinary background in business and human rights during the Business and Human Rights Young Researchers Summit in 2020 in Geneva.

In terms of scope, the framework addresses broadly adverse human rights impacts in the context of Industry 4.0. Due to the interconnectedness of stakeholders in Industry 4.0 by strong technological and organizational links, it is argued that the dependencies in their supply networks could be used to incentivize higher levels of awareness and compliance with the Guiding Principles and, consequently, lead to the emergence of collaborative due diligence processes tailored to the needs of each specific industry involved in Industry 4.0.

The framework is intended to contribute to dealing with the challenges of ongoing fragmentation of regulation in the field of business and human rights, particularly in the EU. The recent disappearance of the proposed EU Directive on Corporate Due Diligence and Corporate Accountability[88] from the legislative agenda[89] sent a message that a comprehensive and overarching due diligence legislation in the EU is nowhere close to be seen. Concomitantly, further development of existing and new national regimes dealing with corporate due diligence and corporate accountability across EU Member States is a clear indicator that, for the time being, Member States will have to deal with issues of corporate accountability in the broader (albeit soft) framework of the Guiding Principles. The risk of keeping national regimes for too long is the ensuing regulatory fragmentation and regulatory burden on companies that operate across more than one jurisdictions in the EU. At the same time, it is an opportunity for the EU to take some distance and only intervene once these regimes have matured, creating a level playing field based on empirical observation. Against this backdrop, the proposed framework intertwines existing legal obligations for due diligence in certain specific domains (e.g., due diligence for data protection, due diligence in export control of dual use items etc.) with a voluntary process of collective due diligence implemented at the level of the business processes of the involved supply chain actors. It offers a roadmap for what States and businesses need to consider in order to discharge their responsibility to protect (for States) and respect (for businesses) human rights in light of the specifics of Industry 4.0.

4.1. Obligations of states with a standard of due diligence

The first building block refers to the obligations of States with a standard of due diligence. It is therefore linked to the first pillar of the Guiding Principles.

In international human rights law, States have three broad categories of obligations, namely obligations to respect, to protect and to fulfil. Obligations to respect may be violated when a State prioritises interests of business entities over internationally protected human rights without proper justification or where it pursues policies which have adverse impact on such rights.[90] Obligations to protect may be violated where States fail to prevent effectively reasonably foreseeable infringements.[91] Finally, obligations to fulfil may be breached where States fail to take steps to make available resources or promote the enjoyment of protected rights.[92] These obligations apply both within a State's territory and extraterritorially in situations over which States exercise control.[93]

In the context of business activities, States can be held directly responsible for the (in)actions of business enterprises in three main cases: (1) if the enterprise is acting on the State's instructions or under

[83] Colin Raffel, *A Call to Build Models Like We Build Open-Source Software*, December 08, 2021, available at: <https://colinraffel.com/blog/a-call-to-build-models-like-we-build-open-source-software.html?s = 09> accessed 28 February 2022.

[84] The recent discovery of the vulnerability in the open source logging library Apache Log4j clearly showed the need of collaborative action in order to make sure that open source software that is critical to virtually every industry remains secure. In the wake of the discover, the White House cybersecurity leader Anne Neuberger organized a meeting with big technological companies and organizations involved in open source software to discuss a sustainable and secure future for open source projects that are critical not only to business but also to national security. Similar thinking could be applied to machine learning models that may become equally critical over time. See Vaughan-Nichols SJ, 'Open Source Security at the White House' (*The New Stack*, 18 January 2022) <https://thenewstack.io/open-source-security-at-the-white-house/> accessed 11 February 2022.

[85] This is a possibility hinted at by the Guiding Principles. See United Nations Human Rights Council (n 1), Principle 30.

[86] Secure Collaborative Intelligent Industrial Automation (SeCoIIA) project, Horizon 2020, Grant Agreement No 871967, available at: <https://secoiia.eu/> accessed 28 February 2022.

[87] SeCoIIA Accountability Workshop, 26 May 2021, available at: <https://secoiia.eu/?tribe_events=secoiia-accountability-workshop> accessed 28 February 2022.

[88] European Parliament, Resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability [2021] (2020/2129(INL)).

[89] Louise Vytopil, 'Human Rights Due Diligence in Supply Chains' (*KPMG*, 10 December 2021) <https://home.kpmg/nl/en/blogs/home/posts/2021/12/human-rights-due-diligence-in-supply-chains.html> accessed 11 February 2022.

[90] United Nations Economic and Social Council (n 47) para 12.

[91] ibid 14.

[92] ibid 23.

[93] ibid 10.

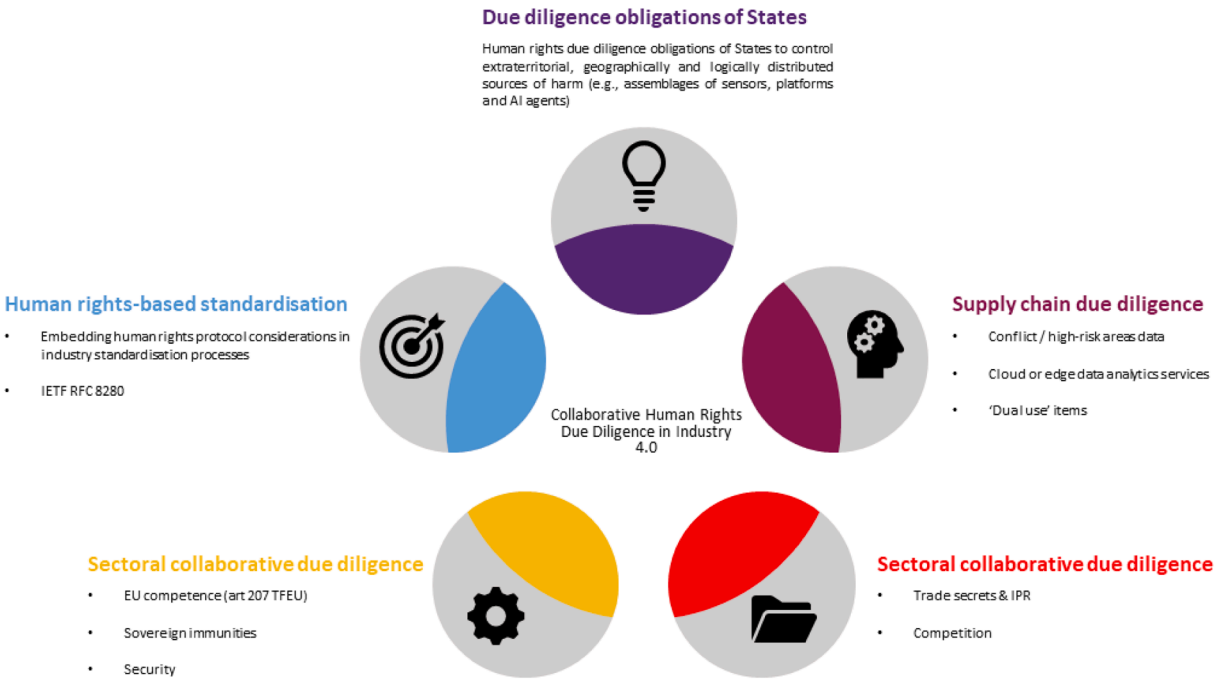

Fig. 1. Collaborative human rights due diligence.

its control or direction; (2) if the enterprise is empowered by a State's law to exercise elements of governmental authority; (3) if the State adopts or acknowledges an enterprise's conduct as its own.[94]

States can also be held indirectly responsible for violations which reveal a failure on their part to take reasonable measures to prevent the occurrence of the event.[95] This is the responsibility of States for failure to act with a standard of due diligence and is also referred to as responsibility for negligence.

The standard of due diligence in international law operates first and foremost in an interstate context. The underlying rationale of due diligence is to ensure the protection of a neighbouring sovereign from the consequences of activities carried out under its own sovereignty, by demonstrating the effectiveness of its powers which are otherwise necessary to fulfil interstate obligations.[96] Due to the particular role of due diligence in international human rights law, however, in this subfield the standard also protects the rights of individuals.

In the framework of collaborative human rights due diligence, the due diligence obligations of States play a critical role as a first step in the protection of human rights. The obligations of States with a standard of due diligence operate in relation to the territory of the State. Thus, the standard is a corollary of the effective power of States to prevent certain activities from taking place on their territory or to ensure their territory is not being used in a way detrimental to the rights and interests of other States. Furthermore, it is well established that certain obligations to prevent are not limited territorially.[97] Indeed, as confirmed by the UN Committee on Economic, Social and Cultural Rights, "[*t*]he extraterritorial obligation to protect requires States (…) to take steps to prevent and redress infringements (…) that occur outside their territories due to the activities of business entities over which they can exercise control (…)".[98]

Thus, in the context of collaborative smart manufacturing in Industry 4.0, international obligations with a standard of due diligence in human rights law should be reconsidered from the perspective of a State's capacity to control extraterritorially, geographically and logically distributed sources of harm. These sources of harm may be both activities of private actors, such as business enterprises, and also actions of artefacts with autonomous decision-making capabilities. Thus, recollecting due diligence obligations of States as part of a State's duty to protect human rights from adverse impacts caused by business activities is a necessary first step to put to work the capacity of the State apparatus.

4.2. *Supply chain due diligence*

The second building block concerns supply chain due diligence. Essentially, this building block refers to mechanisms for ensuring end-to-end transparency of supply chain operations, especially in the context of Industry 4.0.

This building block should include mandatory supply chain due diligence obligations for 'conflict data' which may originate from conflict or high-risk areas. At EU level there are already some examples of such mandatory due diligence exercises in the area of illegal logging and trade in timber,[99] non-financial reporting,[100] data protection,[101] and

[94] ibid 11.
[95] ibid 32.
[96] Hélène Raspail, 'Due diligence et droits de l'homme' [2018] Le standard de due diligence et la responsabilité internationale : Journée d'études du Mans 109.
[97] This is notably the case of prevention and punishment of the crime of genocide, as confirmed by the International Court of Justice in *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment* [2007] ICJ Reports (2007) 43 (International Court of Justice) [153].
[98] United Nations Economic and Social Council (n 47) para 30.
[99] Regulation (EU) No 995/2010 of the European Parliament and of the Council of 20 October 2010 laying down the obligations of operators who place timber and timber products on the market [2010] OJ L.
[100] Directive 2014/95/EU of the European Parliament and of the Council of 22 October 2014 amending Directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups [2014] OJ L 32014L0095.
[101] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L.

conflict minerals.[102] Furthermore, in a number of States there have been similar initiatives at national level, the most prominent being the French Duty of Vigilance Law.[103]

These already existing mandatory due diligence regimes are of particular importance for two reasons. First, they are most likely going to continue to exist on European level as *lex specialis* even after the adoption of the (now defunct) Directive on Corporate Due Diligence and Corporate Accountability.[104] Second, we can already identify some problematic areas that can be equally or more problematic in the complicated setting of smart manufacturing.

Taking data protection as a use case and having in mind that the General Data Protection Regulation (GDPR) does not refer to 'due diligence' as such, the obligations it imposes on data controllers effectively constitute a far-reaching due diligence exercise. For example, as part of the accountability principle under art. 6, data controllers are required to maintain records of processing activities under their responsibility.[105] Importantly, they are also required, where a type of processing in particular using new technologies is likely to result in a high risk to the rights and freedoms of natural persons, to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (article 35). In doing so, they must take into account the nature, scope, context and purposes of the processing, ie the entire operational context. While the GDPR recognises relationships of collaboration through the mechanisms of joint controllership (article 26) and controller-processor arrangements (article 28), it does not contain an elaborate process for data supply chain due diligence.[106]

Against this backdrop, the risks to the rights and freedoms of data subjects may often originate from sources in the data supply chain that are beyond the controller's reach. In the absence of any tangible incentives for collaborative identification and mitigation of risks to the rights and freedoms of data subjects in the GDPR, these challenges would need to be addressed by an umbrella collaborative human rights due diligence process which this article advocates. This would be particularly relevant in the context of collaborative smart manufacturing characterised by higher levels of personalisation and customisation of products and services which would undoubtedly entail processing of data falling within the material scope of the GDPR.[107]

Returning to existing obligations under national law, Savourey and Brabant pinpoint the issues with the scope of the French Duty of Vigilance Law and the scope of the vigilance plan.[108] Furthermore they zoom in on some rather expected concerns related to the vigilance obligations such as lack of clearance on the expected level of detail of a vigilance plan, robustness of risk assessment methodology, etc.[109]

To summarise, while the existing on EU level mandatory due diligence laws reveal certain weaknesses,[110] they also promote a culture of accountability amongst businesses in general as well as in specific industries. Therefore, there is a case for a similar mandatory obligation of due diligence of supply chains in Industry 4.0. It should be imposed not as an individual but as a sector-based shared obligation by means of a duty to cooperate. This obligation should be aimed at enhancing the end-to-end transparency of the supply chain. It should target not only 'conflict data' but also the procurement of cloud or edge analytics services by actors in Industry 4.0. These obligations should be aligned also with ongoing initiatives in export control regulation of dual use items, which have an increased focus on awareness obligations of exporters for items that are or may be intended for use in connection with a violation of human rights, democratic principles or freedom of speech.[111]

4.3. Sectoral collaborative due diligence

The third building block concerns sectoral collaborative human rights due diligence. It lies at the heart of the framework of collaborative human rights due diligence and has two elements which account, respectively, for the public and private aspects.

Sectoral collaborative due diligence works in tandem with supply chain due diligence. The idea is to allow for the equal distribution of control over the possible adverse human rights impacts. Indeed, the characteristics of collaborative smart manufacturing in Industry 4.0 suggest that, above and beyond individual risks, there might be aggregate human rights risks which need to be tackled at the level of the ecosystem.[112] The idea of sectoral collaborative due diligence, thus, suggests that any single actor will have the capacity to identify and assess adverse human rights impacts and to prevent and mitigate either individually or collectively by exercising influence as a group belonging to the same sector of industry.

To be clear, sectoral collaborative due diligence goes beyond mere identification of risks along the supply chain. This is the task of the supply chain due diligence in the second building block. Rather, sectoral collaborative due diligence aims to set out substantive risk-based obligations of conduct for the actors in Industry 4.0. Such a set of obligations could be enshrined in an instrument modelled after the EU General Data

[102] Regulation (EU) 2017/821 of the European Parliament and of the Council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas [2017] OJ L.

[103] Sandra Cossart, Jérôme Chaplier and Tiphaine Beau De Lomenie, 'The French Law on Duty of Care: A Historic Step Towards Making Globalization Work for All' (2017) 2 Business and Human Rights Journal 317.

[104] European Parliament resolution of 10 March 2021 with recommendations to the Commission on corporate due diligence and corporate accountability [2021] (2020/2129(INL)), Recital 15.

[105] Regulation (EU) 2016/679 (n 101), article 30, recital 82.

[106] See on the different modes of collaboration Brendan Van Alsenoy (ed), 'Allocation of Responsibility', *Data Protection Law in the EU: Roles, Responsibilities and Liability*, vol 6 (Intersentia 2019) 76–79 <https://www.cambridge.org/core/books/data-protection-law-in-the-eu-roles-responsibilities-and-liability/allocation-of-responsibility/E4F37D0DC17526B2CE81E43D6F800CE2> accessed 2 April 2021.

[107] See on the ever-growing scope of data protection law Nadezhda Purtova, 'The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law' (2018) 10 Law, Innovation and Technology 40, 41–43.

[108] Elsa Savourey and Stéphane Brabant, 'The French Law on the Duty of Vigilance: Theoretical and Practical Challenges Since Its Adoption' (2021) 6 Business and Human Rights Journal 141, 142–144.

[109] ibid 148.

[110] McCorquodale and others (n 30) 202.

[111] See critique of the approach to the due diligence obligations in the recast of dual-use regulation inMachiko Kanetake, 'The EU's Export Control of Cyber Surveillance Technology: Human Rights Approaches' (2019) 4 Business and Human Rights Journal 155, 158, 161.

[112] For example, in cases of enterprises deploying collaborative robots in different production sites, transfer learning, where knowledge is transferred from one machine learning model to another, may reproduce (unknown) bias and flaws across an extended value chain. In the absence of collaborative due diligence, these risks and their origin can hardly be identified or mitigated by individual companies alone.

Protection Regulation, which combines risk-based substantive obligations with due diligence transparency obligations.[113]

Furthermore, adoption of sectorial collaborative due diligence would facilitate the establishment and implementation of 'multi-stakeholder grievance mechanisms,' reinforcing improving the accessibility and effectiveness of the right to remedy for the potential victims of adverse impacts on human rights. On EU level the proposed Directive on Corporate Due Diligence and Corporate Accountability firmly adopted this approach in its articles 9 and the recital 46.

4.4. Human rights-based standardisation

The fourth and final building block refers to the need of promoting human rights-based standardisation for Industry 4.0 as a way to ensure a uniform approach. While there are already standards tackling various aspects of standardisation in Industry 4.0,[114] none of them accounts for the possible human rights implications.

Early attempts at embedding human rights considerations into technical protocols and architectures could be found in the Internet Engineering Task Force's[115] RFC 8280 titled "Research into Human Rights Protocol Considerations".[116] These efforts should be promoted widely across the Industry 4.0 community and work should be initiated into embedding human rights consideration into technical protocols and reference architecture models.

Reference architecture models play a critical role as they "represent a common structure and language to describe and specify system architectures and, therefore, are beneficial to promote common understanding and system interoperability".[117] Creating a system architecture could be defined as a top-down process of conversion and conceptualisation of customer requirements into an operational concept and design that meet those requirements satisfactorily. System architectures are usually needed when a system is complex or unprecedented,[118] as is clearly the case for smart manufacturing systems.

While there are many reference architecture models for smart manufacturing,[119] so far there has been, to the best of our knowledge, only one attempt to create a legal reference model, namely JuRAMI 4.0.[120] The idea of creating this reference model is to "overcome the gap between the technical and legal domains by visualising the existing problems in their contexts".[121] By using a familiar reference model for Industry 4.0, that is RAMI 4.0, JuRAMI "aims to create a legal reference model that should help viewers to link the familiar with the unfamiliar and hence to gain new insights into previously foreign specialist fields".[122]

While JuRAMI focuses on a limited number of legal domains (eg, civil law, criminal law, data protection law, work safety law and intellectual property law), similar reference architecture models could be created on the basis of human rights considerations. Reference models "provide a framework for the standardization of relevant technical systems, from development, through integration, to operation".[123]As a minimum, these should cover aspects of collaborative autonomous decision-making, cybersecurity as a guarantee for human rights protection in collaborative smart environments, end-to-end transparency of cyber-physical supply networks, dynamic predictive risk analysis of potential adverse human rights impacts, and usage of information and operational technology forensics for accountability purposes. Ultimately, the proliferation of such reference models could not only raise awareness amongst the smart manufacturing community but may also drive standardisation in the field.

4.5. Limitations of the blueprint

It must be acknowledged that the proposed blueprint has certain limitations. First, there is a risk that this blueprint could be seen as a 'one-size-fits-all' methodology for states and businesses to address every concern pertaining to adverse human rights impacts in Industry 4.0. This is not the goal. Instead, the framework aims to provide a set of steps that both states and businesses need to take in order to discharge their human rights due diligence duties in the context of the challenges of Industry 4.0.

Second, there is a tangible concern relating to the implementation of the proposed collaborative due diligence process on the part of businesses. Our experience in the SeCoIIA project has shown that there are considerable issues pertaining to interoperability of legacy and new systems, which is a common scenario in safety- and security-conservative industries, such as manufacturing. Effectively, this means that companies may struggle to share operational and organizational data pertaining to their business processes, which is a prerequisite for any type of a collaborative due diligence exercise. Furthermore, companies themselves tend to be wary of sharing commercially sensitive data beyond the absolute minimum and our experience in SeCoIIA has shown that this is, somewhat surprisingly, the case even where companies see each other as a trustworthy partner. While some of these concerns are only perceived, any collaborative due diligence process must be backed by clear contractual arrangements as to the type, volume, quality, and frequency of commercially sensitive data sharing for

[113] See, among others, Regulation (EU) 2016/679 (n 101), articles 13-14, 35-36.

[114] For example, Reference Architecture Model for Industry 4.0 (RAMI4.0), The Industrial Internet Reference Architecture v 1.9, IDS-RAM 3.0, ISO/IEC JTC1 Meta Reference Architecture and Reference Architecture for System Integration, ISO/TC 184 – IEC/TC 65 Joint Working Group 21 Smart Manufacturing Meta-Model "A Meta-modelling analysis approach to Smart Manufacturing Reference Models (SMRM)", ISO/IEC JTC 1 SC41 Internet of Things and related technologies Reference Architecture for IoT, ISO/IEC JTC 1/SC 41/AG 20 Sectorial Liaison Group (SLG 1) on Industrial IoT (IIoT) Standard mapping for reference architecture models.

[115] The Internet Engineering Task Force is an "open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet" and it is "the premier Internet standards body, developing open standards through open processes". See more at: https://www.ietf.org/about/

[116] Niels ten Oever and Corinne Cath, RFC 8280 'Research into Human Rights Protocol Considerations' 2017. See for a recent commentary Vivek Krishnamurthy, 'Are Internet Protocols the New Human Rights Protocols? Understanding "RFC 8280 – Research into Human Rights Protocol Considerations"' (2019) 4 Business and Human Rights Journal 163.

[117] Francisco Fraile and others, 'Reference Models for Digital Manufacturing Platforms' (2019) 9 Applied Sciences 4433, 2.

[118] Alexander Levis, 'System Architectures' in Andrew P Sage and William B Rouse (eds), *Handbook of Systems Engineering and Management* (Second Edition, John Wiley & Sons 2014) 479.

[119] For an overview of some of them, see Moghaddam and others (n 4) 217–220.

[120] Eric Hilgendorf and Uwe Seidel, 'Legal Challenges Facing Digital Value Chains – Structured Solution Paths for SMEs' (2016) 8–10.

[121] ibid 5.

[122] ibid.

[123] Fraile and others (n 117) 2.

the purposes of the due diligence exercise.

Finally, the framework, and specifically its sectoral collaborative due diligence block, has the same weaknesses of any non-binding instrument and, recursively, it is the fact that it is non-binding. We believe, however, that the inevitable network-wide structural, logical and organizational dependencies created by the horizontal, vertical and end-to-end integration in Industry 4.0 would incentivize companies to be more open and to work collectively on a problem that should be their common concern.

4.6. Beyond the blueprint

The blueprint should not be perceived in isolation from other approaches to dealing with adverse human rights impacts and, more broadly, socio-economic harm. To the contrary, our proposal is intended to be interoperable with other methodologies for socio-economic impact assessment of new and emerging technologies.[124] Our proposed blueprint shares a lot of commonalities with the general principles for socio-economic impact assessments reported in literature, such as comprehensiveness, openness and inclusiveness, proportionality and reliance on evidence, transparency, bias mitigation and flexibility and adaptivity, and equitability.[125] Indeed, collaborative human rights due diligence is a complementary tool to such assessments and one that could both feed on insights from socio-economic perspective and serve as an add-on to socio-economic assessment.[126]

The blueprint also aims to support broader accountability mechanisms for socio-technical systems such as smart manufacturing. Recent interdisciplinary research has demonstrated that goal-driven architectures could utilize causality to reason about accountability in such socio-technical systems.[127] Accountability could be thought of as a "property of a system that helps to identify the causes of (unwanted) events related to a quality attribute".[128] Thus, enabling accountability entails the development of a system with forensic capabilities that can support the identification of misbehaving parties and linking their conduct with specific violations.[129] In this context, accountability is seen as a "a technical component that employs automated causal reasoning and logging to aid, stakeholders within a specific socio-technical context, in determining responsible parties for specific observations".[130] The goal-driven architecture is proposed in recognition of the fact that modelling a system-wide accountability mechanism capable of explaining all events in a system is futile due to its complexity and prohibitive costs.[131] Therefore, it is more practical to construct accountability mechanisms in relation to concrete accountability goals that define the socio-technical environment, as a "property from the domain of a quality concern, that serves as the functionality of the technical component".[132]

Acknowledging that formalisation of a notion of accountability that is equally acceptable to all disciplines is an equally futile undertaking, we subscribe to the view that there is a need for future work at the intersection of accountability in socio-technical systems and the problem of what constitutes a valid model for an accountable system, i.e. what should be the qualities of the causal knowledge so as to enable accountability.[133] We see the blueprint and any practical instantiations of it in the form of due diligence exercises as capable of providing insights into a vast array of use cases and industries to support reasoning about causality-based accountability mechanisms.

5. Conclusion

Collaborative smart manufacturing in Industry 4.0 represents a significant shift in the convention manufacturing paradigm. The vertical and horizontal integration of actors in the supply chain leads to the emergence of new business relationships entailing new potential adverse human rights impacts. It is beyond doubt that business entities have a corporate responsibility to respect human rights. A main tool to discharge this responsibility, human rights due diligence is premised on the idea that it is within the business enterprise's control to prevent or mitigate human rights impacts at the beginning of a new business relationship or activity. This assumption, however, is challenged by technological and organisational processes within Industry 4.0 which are based on complex real-time network interactions and data-driven autonomous decision-making. In this new collaborative environment, the manufacturer becomes one of many actors in a network, along with the customer. This gives rise to new potential aggregate adverse human rights impacts at the level of the ecosystem which cannot be sufficiently addressed by any single actor alone.

This article proposed a blueprint of a four-component framework of collaborative human rights due diligence integrates elements from the three pillars of the Guiding Principles. It is an invitation to scholarly debate on the need of hybrid approaches to human rights due diligence in Industry 4.0. By adopting a hybrid approach to human rights due diligence, this framework aims to incentivise the actors in the manufacturing supply network of particular industries, such as aerospace, to pool their due diligence efforts. While sharing the costs and benefits, such a framework could have long-run spillover effects of nudging businesses to collaborate also on providing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research is funded by the European Union's Horizon 2020 research and innovation programme under the Secure Collaborative Intelligent Industrial Automation (SeCoIIA) project, grant agreement No 871967. The authors have contributed equally to this work. The authors would like to thank Dr Anil Yilmaz-Vastardis for her insightful comments on earlier drafts of this paper and suggestions for improvement and future research. As always, any errors or oversights are ours alone.

[124] Rowena Rodrigues and Martina Diez Rituerto, 'Socio-Economic Impact Assessments for New and Emerging Technologies' (2022) 9 Journal of Responsible Technology 100019, 1.

[125] ibid 4.

[126] ibid 10.

[127] Amjad Ibrahim, Stavros Kyriakopoulos and Alexander Pretschner, 'Causality-Based Accountability Mechanisms for Socio-Technical Systems' (2021) 7-8 Journal of Responsible Technology 100016, 2.

[128] ibid 2.

[129] ibid

[130] ibid 3.

[131] ibid

[132] ibid

[133] ibid 11.

Further reading

Aho, B., & Duffield, R. (2020). Beyond Surveillance capitalism: privacy, regulation and big data in Europe and China. *Economy and Society, 49*, 187.

Alcácer, V., & Cruz-Machado, V. (2019). Scanning the industry 4.0: A literature review on technologies for manufacturing systems. *Engineering Science and Technology, an International Journal, 22*, 899.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro). (2007). *Judgment [2007] ICJ Reports, 43* (International Court of Justice).

Baines, T. S., & others. (2009). The Servitization of Manufacturing: A review of literature and reflection on future challenges. *Journal of Manufacturing Technology Management, 20*, 547.

Bécue, A., Praça, I., & Gama, J. (2021).'Artificial intelligence, cyber-threats and industry 4.0: Challenges and opportunities' *Artificial Intelligence Review*<10/gjxhdv> accessed 9 May 2021.

Bonnitcha, J., & McCorquodale, R. (2017a). The concept of "due diligence" in the UN guiding principles on business and human rights. *European Journal of International Law, 28*, 899.

Bonnitcha, J., & McCorquodale, R. (2017b). The concept of "due diligence" in the UN guiding principles on business and human rights: A rejoinder to John Gerard Ruggie and John F. Sherman, III'. *European Journal of International Law, 28*, 929.

Cabrelli, D., & Graveling, R. (2019). Health and safety in the workplace of the future. *Briefing PE, 638*, 434. https://op.europa.eu/en/publication-detail/-/publication/e2f19fe1-e32d-11e9-9c4e-01aa75ed71a1/language-en.

Commission Recommendation (EU). (2019). Cybersecurity of 5G networks.] *OJ L, 88*.

Cossart, S., Chaplier, J., & Beau De Lomenie, T. (2017). The French law on duty of care: A historic step towards making globalization work for all. *Business and Human Rights Journal, 2*, 317.

De Schutter, O. (2012).and others, 'Human rights due diligence: the role of states'.

Dheu, O., Ducuing, C., & Valcke, P. (2020). The emperor's new clothes: A roadmap for conceptualizing the new vehicle.] *TRANSIDIT, 12*.

Directive 2014/95/EU of the European parliament and of the council of 22 october 2014 amending directive 2013/34/EU as regards disclosure of non-financial and diversity information by certain large undertakings and groups (2014). [32014L0095].

European Commission, 'Smart manufacturing' (Shaping Europe's digital future - European commission, 8 august 2018) https://ec.europa.eu/digital-single-market/en/smart-manufacturing accessed 23 March (2020).

European Commission, Proposal for a directive of the European parliament and of the council on measures for a high common level of cybersecurity across the union, repealing directive (EU) 2016/1148 [(2020).] COM/2020/823 final.

European Commission 'White paper on artificial intelligence—A European approach to excellence and trust' COM (2020). 65 final, 19.02.2020.

European Parliament, Resolution of 10 March 2021 with recommendations to the commission on corporate due diligence and corporate accountability [(2021).] (2020/2129(INL)).

Fasterling, B. (2017). Human rights due diligence as risk management: Social risk versus human rights risk. *Business and Human Rights Journal, 2*, 225.

Fraile, F., & others. (2019). Reference models for digital manufacturing platforms. *Applied Sciences, 9*, 4433.

Gebru, T. (2020).and others, 'Datasheets for Datasets']arXiv:1803.09010 [cs] http://arxiv.org/abs/1803.09010 accessed 2 April 2021.

General Comment No. 24 (2017). On state obligations under the international covenant on economic, social and cultural rights in the context of business activities 2017 [E/C.12/GC/24].

Gerrikagoitia, J. K., & others. (2019). Digital manufacturing platforms in the industry 4.0 from private and public perspectives. *Applied Sciences, 9*, 2934.

Harrison, J. (2011). Human rights measurement: reflections on the current practice and future potential of human rights impact assessment. *Journal of Human Rights Practice, 3*, 162.

Harrison, J. (2013). Establishing a meaningful human rights due diligence process for corporations: learning from experience of human rights impact assessment. *Impact Assessment and Project Appraisal, 31*, 107.

Hilgendorf, E., & Seidel, U. (2016).'Legal challenges facing digital value chains – Structured solution paths for SMEs'.

Hofmann, H., Schleper, M. C., & Blome, C. (2018). Conflict minerals and supply chain due diligence: An exploratory study of multi-tier supply chains. *Journal of Business Ethics, 147*, 115.

Hon, W. (2017). *Data localization laws and policy*. Edward Elgar Publishing. https://www.elgaronline.com/view/9781786431967.xml accessed 25 February 2020.

Ibrahim, A., Kyriakopoulos, S., & Pretschner, A. (2021). Causality-based accountability mechanisms for socio-technical systems. *Journal of Responsible Technology, 7-8*, Article 100016.

International Federation for Human Rights, Amesys case: The investigation chamber green lights the investigative proceedings on the sale of surveillance equipment by Amesys to the Khadafi regime, 17 January (2013)., available at: Https://www.refworld.org/docid/511cb668a.html.

Kanetake, M. (2019). The EU's export control of cyber surveillance technology: Human rights approaches. *Business and Human Rights Journal, 4*, 155.

Klarman, S., Schlobach, S., & Serafini, L. (2012). Formal verification of data provenance records. *The Semantic Web – ISWC 2012, Lecture Notes in Computer Science*, 215–230.

Kott, A. (2019). Intelligent autonomous agents are key to cyber defense of the future army networks.] *The Cyber Defense Review, 57*.

Kriebitz, A., & Lütge, C. (2020). Artificial intelligence and human rights: A business ethical assessment. *Business and Human Rights Journal, 1*.

Krishnamurthy, V. (2019). Are internet protocols the new human rights protocols? Understanding "RFC 8280 – Research into human rights protocol considerations. *Business and Human Rights Journal, 4*, 163.

Levis, A. (2014). System architectures. In Andrew P. Sage, & William B. Rouse (Eds.), *Handbook of systems engineering and management*. John Wiley & Sons. Second Edition.

Li, C. (2020). *OpenAI's GPT-3 language model: A technical overview*. Lambda Labs. June 03, available at: Https://lambdalabs.com/blog/demystifying-gpt-3/.

Martin, R.A. (. 2020).'Visibility & control: Addressing supply chain challenges to trustworthy software-enabled things']*2020 IEEE Systems Security Symposium (SSS)*<10/gjmztw>.

McCorquodale, R., & others. (2017). Human Rights due diligence in law and practice: Good practices and challenges for business enterprises. *Business and Human Rights Journal, 2*, 195.

McFarlane, D. (2018).'Industrial internet of things: applying IoT in the industrial context' https://www.ifm.eng.cam.ac.uk/uploads/DIAL/industrial-internet-of-things-report.pdf.

McFarlane, D. (2020). *Factories of the future and implications for automation*. University of Cambridge, Institute for Manufacturing Insights. https://www.ifm.eng.cam.ac.uk/insights/automation/factories-of-the-future-and-implications-for-automation/ accessed 11 March.

Methven O'Brien, C., & Dhanarajan, S. (2016). The corporate responsibility to respect human rights: A status review. *Accounting, Auditing & Accountability Journal, 29*, 542.

Mittal, S., & others. (2019). Smart manufacturing: characteristics, technologies and enabling factors. *Proceedings of the Institution of Mechanical Engineers, Part B: Journal of Engineering Manufacture, 233*, 1342.

Moghaddam, M., & others. (2018). Reference architectures for smart manufacturing: A critical review. *Journal of Manufacturing Systems, 49*, 215.

Moore, P. (2020).'Study on data subjects, digital surveillance, AI and the future of work' Study addressed to, the members and staff of the European parliament as background material to assist them in their parliamentary work https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf.

National Institute of Standard and Technology, 'Smart manufacturing operations planning and control' (2014). https://www.nist.gov/system/files/documents/2017/05/09/FY2014_SMOPAC_ProgramPlan.pdf accessed 17 November 2020.

Nollkaemper, A. (2015).'The problem of many hands in international law' Amsterdam law school legal studies research paper https://dare.uva.nl/search?sort=year;field1=dai;value1=075187744;docsPerPage=1;startDoc=32 accessed 7 February 2020.

Oever, N ten, & Cath, C. (2017).RFC 8280 'research into human rights protocol considerations'.

Office of the UN High Commissioner for Human Rights, 'The corporate responsibility to respect human rights: An interpretive guide' (2012). HR/PUB/12/02 https://www.ohchr.org/Documents/publications/hr.puB.12.2_en.pdf accessed 24 March 2020.

'Operational Technology (OT)' (Gartner glossary) https://www.gartner.com/en/information-technology/glossary/operational-technology-ot accessed 24 March (2020).

Peng, S. (2020). A new trade regime for the servitization of manufacturing: Rethinking the goods-services dichotomy. *Journal of World Trade, 54*. http://kluwerlawonline.com/journalarticle/Journal+of+World+Trade/54.5/TRAD2020030 accessed 17 November 2020.

Pisillo Mazzeschi, R. (2018). Le chemin étrange de la due diligence: D'un concept mystérieux à un concept surévalué. In Sarah Cassella (Ed.), *Le standard de due diligence et la responsabilité internationale: Journée d'études franco-italienne du mans*. Éditions A Pedone.

Purtova, N. (2018). The law of everything. broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology, 10*, 40.

Raffel, C., & Call to, A. (2021).Build models like we build open-source software, December 08,, available at: Https://colinraffel.com/blog/a-call-to-build-models-like-we-build-open-source-software.html?s=09.

Raidman, D. (2021).'Why we need a software bill of materials industry standard' (DevOps.com, 20 August 2020) https://devops.com/why-we-need-a-software-bill-of-materials-industry-standard/ accessed 2 April.

Raspail, H. (2018).'Due diligence et droits de l'homme'] Le standard de due diligence et la responsabilité internationale : Journée d'études du mans.

Regulation (EU) No 995/2010 of the European parliament and of the council of 20 October 2010 laying down the obligations of operators who place timber and timber products on the market text with EEA relevance (2010). (OJ L).

Regulation (EU) 2016/679 of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (2016). (OJ L).

Regulation (EU) 2016/679 of the European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) (2016). (OJ L).

Regulation (EU) 2017/821 of the European Parliament and of the council of 17 May 2017 laying down supply chain due diligence obligations for Union importers of tin, tantalum and tungsten, their ores, and gold originating from conflict-affected and high-risk areas (2017). (OJ L).

Regulation (EU) 2021/821 of the European Parliament and of the council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast) [(2021).]OJ L 206.

Rodrigues, R., & Rituerto, M. D. (2022). Socio-economic impact assessments for new and emerging technologies. *Journal of Responsible Technology, 9*, Article 100019.

Ruggie, J. G. (2014). Global governance and "new governance theory": Lessons from business and human rights. *Global Governance: A Review of Multilateralism and International Organizations, 20*, 5.

Ruggie, J. G. (2018). Multinationals as global institution: power, authority and relative autonomy: Multinationals as global institution'. *Regulation & Governance, 12*, 317.
Ruggie, J. G., & Sherman, J. F. (2017). The concept of "due diligence" in the UN Guiding principles on business and human rights: A reply to Jonathan Bonnitcha and Robert McCorquodale. *European Journal of International Law, 28*, 921.
Savourey, E., & Brabant, S. (2021). The French law on the duty of vigilance: Theoretical and practical challenges since its adoption. *Business and Human Rights Journal, 6*, 141.
SeCoIIA Accountability Workshop, 26 May (2021)., available at: Https://secoiia.eu/?tribe_events=secoiia-accountability-workshop.
Secure Collaborative Intelligent Industrial Automation (SeCoIIA) project, Horizon (2020)., Grant Agreement No 871967, available at: Https://secoiia.eu/.
Smit, J. (2016).and others, 'Industry 4.0′ Study IP/A/ITRE/2015-02 https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf accessed 12 March 2020.
Smit, L. (2020).and others, Study on due diligence requirements through the supply chain: Final report. https://op.europa.eu/publication/manifestation_identifier/PUB_DS0120017ENN accessed 7 August 2020.
Struth, W. (2015)'Data is key raw material for industry 4.0′ (Bosch ConnectedWorld Blog, 10 June. https://blog.bosch-si.com/industry40/data-key-raw-material-for-industry-40/ accessed 2 April 2021.
Taka, M. (2016). Emerging practice in responsible supply chain management: Closed-Pipe supply chain of conflict-free minerals from the democratic Republic of Congo. *Business and Society Review, 121*, 37.
Thompson, D. F. (2014). Responsibility for failures of government: The problem of many hands. *The American Review of Public Administration, 44*, 259.
United Nations Human Rights Council, Protect, respect and remedy: A framework for business and human rights (2008).
United Nations Human Rights Council, 'Guiding principles on business and human rights' (2011). [A/HRC/17/31].
Van Alsenoy, B (Ed.). (2019). Allocation of Responsibility. *Data Protection Law in the EU: Roles, Responsibilities and Liability, 6*. Intersentia https://www.cambridge.org/core/books/data-protection-law-in-the-eu-roles-responsibilities-and-liability/allocation-of-responsibility/E4F37D0DC17526B2CE81E43D6F800CE2 accessed 2 April 2021.
Vaughan-Nichols, S.J. (.2022))'Open source security at the white house' (The New Stack, 18 January. https://thenewstack.io/open-source-security-at-the-white-house/.
Vytopil, L. (2021))'Human rights due diligence in supply chains' (KPMG, 10 December. https://home.kpmg/nl/en/blogs/home/posts/2021/12/human-rights-due-diligence-in-supply-chains.html.
Wyggers, K. (2020).OpenAI launches an api to commercialize its research, Venture Beat, June 11,, available at: Https://venturebeat.com/2020/06/11/openai-launches-an-api-to-commercialize-its-research/.
Zerk, J.A. (.2010).'Extraterritorial jurisdiction: Lessons for the business and human rights sphere from six regulatory areas' Working Paper No. 59 https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/programs/cri/files/workingpaper_59_zerk.pdf accessed 2 April 2021.

Practising lawyer and doctoral researcher in IP law and computer science at the Centre for IT & IP Law at KU Leuven, Belgium. He has a background and professional experience in computer science and systems programming. In his research, he is exploring the scope and limits of copyright law applicable to machine learning artifacts and its impact on user freedoms granted by free and open source software licenses.

Lawyer and researcher at the Centre for IT & IP Law at KU Leuven, Belgium, specialising in protection of human rights in digital supply chains and in relation to development and deployment of disruptive technologies, particularly artificial intelligence.