Speculum Juris

Vol 38 No 2 (2024)
Published 31 December 2024

ISSN 2523-2177

Cite as: Meyer "Civil Liability for Delicts Caused by Emerging Digital Technology: A Suggestion to South Africa" 2024 (38) Spec Juris 296–335

University of Fort Hare
Together in Excellence

Civil Liability for Delicts Caused by Emerging Digital Technology: A Suggestion to South Africa*

Jacqui Meyer**
Campus Faculty Head: Law at The Independent Institute of Education (The IIE), Varsity College, Pretoria Campus

Abstract

The increasing complexity of emerging digital technologies (EDT) presents challenges for existing legal frameworks, particularly regarding liability for harm caused by EDTs. As EDTs become more autonomous and capable of making decisions without human control, the traditional concept of delict (wrongful act) attributed to human actors is no longer sufficient. Current laws, which require liability on humans or their property (e.g., animals), struggle to address harm caused by autonomous systems. In South Africa, where EDT is not yet regulated, mechanisms such as product liability, vicarious liability, and the actio de pauperie (liability for damage caused by animals) are inadequate for regulating the complexities of EDT-related harm. These frameworks fail to account for situations where damage is caused by non-human autonomous or semi-autonomous technologies, leaving a gap in legal responsibility. In contrast, the European Union (EU) has taken steps to address these challenges. The Artificial Intelligence Act 2024, along with the Product Liability Directive and the Artificial Intelligence Liability Directive, creates a regulatory framework that holds manufacturers or

* This article is a revised version of a paper presented at the 2023 Annual International Mercantile Law Journal hosted by the University of the Free State in October 2023.

** LLM (Labour Law) (UNISA).

operators of AI systems accountable for the harm caused by their technologies. This shift moves away from human accountability alone, focusing instead on responsible management of autonomous systems. This article suggests that South Africa adopt the European model, tailoring it to local needs. By implementing similar frameworks, South Africa can ensure clear accountability for the harm caused by EDT, even when no human actor is directly involved, and create new legal structures to address the evolving nature of technology.

Keywords: delictual liability; electronic entity; emerging digital technology; product liability; vicarious liability; *actio de pauperie*

1 INTRODUCTION

> For most technological ecosystems (by which we mean systems with interacting devices or programs), however, no specific liability regimes exist. This means that product liability, general tort law rules (fault-based liability, tort of negligence, breach of statutory duty), and possibly contractual liability, occupy centre stage. The more complex these ecosystems become with emerging digital technologies, the more increasingly difficult it becomes to apply liability frameworks.[1]

Even for the non-tech savvy, engaging with Artificial Intelligence (AI) and the Internet of Things (IoT) has become imperative to survive in contemporary society. In recent years, one is hard-pressed not to hear about these emerging digital technologies (EDT),[2] considering how much they have dominated public conversations.[3] Artificial Intelligence refers to developing computer systems capable of performing tasks that typically require human intelligence, such as visual perception, decision-making, and speech recognition.[4] The Internet of Things could be understood to mean the connectivity between devices and objects to the internet, allowing

1 Expert Group on Liability and New Technologies – New Technologies Formation "Liability for Artificial Intelligence and Other Emerging Digital Technologies" https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf p17 (accessed 12-06-2022).

2 This term was defined in the Commission Staff Working Document "Liability for Emerging Digital Technologies" SWD/2018/137/final https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52018SC0137 (accessed 12-06-2022). The term "emerging digital technologies" is described as new and rapidly growing breakthrough technologies. The main emerging technologies nowadays are Artificial Intelligence (AI), Internet of Things (IoT), blockchain, big data, cybersecurity, robotics, and virtual reality. See digital sk:// up "What are Emerging Digital Technologies and Why are They Relevant?" https://www.digitalskillup.eu/articles/what-are-emerging-technologies/ (accessed 16-07-2024).

3 Around 2014, the industry experienced another "about turn" with the appearance of smart factories and online production management. Returning to Schwab and his book *The Fourth Industrial Revolution,* the German economist foresaw what was to come: "We are at the beginning of a revolution that is fundamentally changing the way we live, work, and relate to one another. In its scale, scope and complexity, what I consider to be the Fourth Industrial Revolution is unlike anything humankind has experienced before. And this is for three reasons about which the experts agree: Its speed, scope and unprecedented impact." Schwab "The Fourth Industrial Revolution" *Encyclopedia Britannica* 31 May 2023 https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734 (accessed 12-06-2022).

4 BlockChain Council "What is Artificial Intelligence? A Step by Step Beginners Guide" https://www.blockchain-council.org/ai/what-is-artificial-intelligence/?gad_source=1&gclid=Cj0KCQjw-uK0BhC0ARIsANQtgGPjuFPcVBD3EVOTHI3-_ZwOx559xeeVqTGpBYaGKpjbyyK2H4thOHkaAjtMEALw_wcB (accessed 16-07-2024).

for the gathering and extraction of data.[5] These words represent human evolution[6] moving from the Fourth Industrial Revolution (4IR)[7] into the Fifth Industrial Revolution. Emerging digital technologies accomplish many advantages in numerous fields, including the medical, financial and transport industries,[8] presenting economic growth for countries. This is highlighted by companies and policymakers' investments in these fields. Internationally, "[a] Europe fit for the digital age"[9] is one of the primary priorities of the European Union (EU) Commission.[10]

Emerging digital technologies can combine connectivity, autonomy, and data dependency to perform tasks without human control or supervision.[11] Artificial Intelligence-equipped systems can also improve their performance by learning from experience. Their complexity is reflected in the diversity of economic operators involved in the production and supply chain.[12] Despite EDT's benefits, it is crucial to acknowledge and address the potential risks[13] and outstanding

5 BlockChain Council "How is IoT Changing Various Industries?" https://www.blockchain-council.org/ai/how-iot-is-changing-various-industries/?gad_source=1&gclid=Cj0KCQjw-uK0BhC0ARIsANQtgGPt_FEL9HRjSRSeGJd3WA65153iK95_ViC-8dQNoUwlyMxLoCVuN0YaApf3EALw_wcB (accessed 16-07-2024).

6 Humans have witnessed transformative industrial revolutions that reshaped societies and economies from mechanisation (1.0 Mechanisation – The introduction of industrial production equipment driven by water and steam power, recorded from 1780), to electricity (2.0 Electrification – Mass production using electrical energy and assembly lines, dating from 1870) and automation (3.0 Automation – Automated production due to a rise of electronics, telecommunications, and computers, dated from 1970) and mass production (4.0 Digitalisation – dating from 2011, this period concerns the use of cyber-physical systems on connected devices to automate further processing). Some authors believe humanity is already progressing into the Fifth Industrial Revolution, as is expounded by COVID-19 (5.0 Personalisation – the interdependence of man and machine using cognitive computing and human intelligence. Mass customization and personalization for humans (from 2020). Sarfraz, Sarfraz, Iftikarand Akhund "Is COVID-19 Pushing us to the Fifth Industrial Revolution (Society 5.0)?" 2021 *Pakistan Journal of Medical Sciences* 10.12669/pjms.37.2.3387. This is not inconceivable as the modern-day Thomas Edison, Elon Musk's Neuralink company has already implanted a brain-computer interface earlier in 2024, with moderate success. Staff Reporter "Elon Musk says Neuralink will Test Brain Implant on Second Patient in 'Next Week or So'" *The Guardian* (accessed 11-07-2024).

7 Jansen van Rensburg, Telukdarie and Dhamija, "Society 4.0 Applied in Africa: Advancing the Social Impact of Technology" 2019 *Technology in Society* 59 https://doi.org/10.1016/j.techsoc.2019.04.001 (accessed 12-07-2022) explains the "Fourth Industrial Revolution" as a term created in Germany relating to cutting-edge technology activity, innovations, digital physical frameworks, the Internet of Things, and distributed computing.

8 It is estimated that around 90 per cent of road accidents are caused by human errors. See Commission's Report on Saving Lives: Boosting Car Safety in the European Union (EU) COM/2016/0787/final (accessed 12-06-2022).

9 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en (accessed 09-06-2022).

10 The European Union Commission (EU) secured 1,5 billion euro in funding for targeted research and 20 billion euro of total investment in AI annually. https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#:~:text=The%20AI%20strategy%20proposed%20measures,global%20hub%20for%20trustworthy%20AI (accessed 09-06-2022).

11 EUR-Lex "Report from the Commission to the European Parliament, the Council and The European Economic and Social Committee Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics" (the EU AI report) https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52020DC0064 (accessed 12-06-2022).

12 Consumer Protection Act 68 of 2008 (CPA) s 1, defines "supply chain" to mean: "with respect to any particular goods or services, means the collectively of all suppliers who directly or indirectly contribute in turn to the ultimate supply of those goods or services to a consumer, whether as a producer, importer, distributor or retailer of goods, or as a service provider." https://www.gov.za/sites/default/files/gcis_document/201409/321864670.pdf (accessed 12-06-2022).

13 Fox "Human Rights Lawyer Susie Alegre: 'If AI is so Complex it Can't be Explained, There are Areas where it Shouldn't Be Used'" *The Guardian* (11 May 2024) explains that the private-sector technology is being inserted into people's lives to replace human relationships, and that is very dangerous.

concerns, including questions of civil liability.[14] The variety of components, parts, software, systems, or services that together form the new technological ecosystems and their openness to updates and upgrades after their placement on the market poses significant challenges that require careful consideration.

> Along with the opportunities that AI, IoT and robotics can bring to the economy and our societies, they can also create a risk of harm to legally protected interests, both material and immaterial ones. The risk of such harm occurring will increase as the field of applications widens. In this context, it is essential to analyse whether and to what extent the current legal framework on safety and liability is still fit to protect users.[15]

The news easily provides examples of EDT-related fatalities and incidents. The AI Incident Database indexes the collective history of harms or near harms realised by deploying artificial intelligence systems.[16] Over 700 EDT-related incidents have been reported worldwide by the AI Incident database. These range from a husband who committed suicide after having a relationship with an AI model,[17] to a pedestrian dragged under a robot taxi to Tesla's autopilot, causing fatalities and injuries.[18]

As such, member states of the EU have already proposed and approved sector-specific legislation.[19] Most nations within the Organisation of Economic Corporation and Development (OECD) have already developed policies and legislation supporting EDT, making it their preferred vehicle for economic growth and prosperity.[20] However, in South Africa, it is acknowledged that "[t]he economic development trajectory of Africa during the 1st to the 3rd industrial revolutions have always lagged behind those of the Western and Eastern countries".[21] South Africa has not yet drafted or submitted bills to parliament or formalised any policy documents for the regulation

14 The European Council of October 2017 stated that the EU needs a sense of urgency to address emerging trends such as AI "while at the same time ensuring a high level of data protection, digital rights and ethical standards" and invited "the Commission to put forward a European approach to artificial intelligence". The European Parliament made wide-ranging recommendations on civil law rules on robotics and the European Economic and Social Committee has also issued an opinion on the topic. European Parliament Resolution with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)); European Economic and Social Committee Ppinion on AI (INT/806-EESC-2016-05369-00-00-AC-TRA) (accessed 12-06-2022).

15 The EU AI report fn ref 13.

16 AI Incident Database https://incidentdatabase.ai/summaries/incidents/ (accessed 15-06-2024).

17 Sellman "AI Chatbot Blamed for Belgian Man's Suicide" (31 March 2023) *The Times* https://www.thetimes.com/business-money/technology/article/ai-chatbot-blamed-for-belgian-mans-suicide-zcjzlztcc#:~:text=A%20young%20father%20took%20his,apparently%20encouraging%20him%20towards%20suicide (accessed 15-06-2024).

18 Felton and Seal "U.S. Regulators Tie Tesla's Autopilot to More than a Dozen Fatalities, Hundreds of Crashes" *The Wall Street Journal* https://www.wsj.com/business/autos/regulators-probing-tesla-recall-tied-to-autopilot-a1af6d67?mod=hp_lead_pos5 (accessed 15-06-2024).

19 For example, Germany has amended its Street Traffic Act (due to the Justice Ministers of the German federal states adopting a resolution in June 2017 calling for legislative action, including at the EU level as needed, around liability for the operation of AI) to allow autonomous cars to operate on the streets provided that a human driver is present always to take over control. Sweden has introduced a law that will enable the testing of autonomous vehicles. In the UK, the government has proposed legislation that would amend insurance legislation concerning the possible roll-out of autonomous vehicles. In the US, numerous states are addressing the need for legislation on autonomous vehicles, although laws vary widely since they address licensing, use or regulation issues. In Japan, the Ministry of Economy, Trade and Industry discusses legal issues regarding AI from the perspective of rights and responsibilities, including liability. See House of Commons Library "Briefing Paper, Automated and Electric Vehicles Bill 2017-19, 28 November 2017" http://researchbriefings.files.parliament.uk/documents/CBP-8118/CBP-8118.pdf (accessed 12-06-2022).

20 https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (accessed 01-10-2024).

21 Minister Khumbudzo Ntshavheni: Artificial Intelligence Regulation while Encouraging Innovation https://www.gov.za/speeches/minister-khumbudzo-ntshavheni-remarks-artificial-intelligence-ai-regulation-while (Minister Ntshavheni's speech) (accessed 12-06-2022).

of AI.[22]

Drafting civil liability EDT regulation takes work, though. This is premised on four proposed aspects: first, EDT is placed on a spectrum. Second, Bronfenbrenner's ecological systems theory provides that individuals live in a constantly changing context influenced by the relationships between individual contexts and macro systems.[23] Given that the concept of *ubuntu* drives South African constitutionalism,[24] what a South African software programmer of EDT will program into the algorithms of such EDT will, and does, differ from that of another country's software programmer. Therefore, the algorithms from different countries will vary in their reactions to external stimuli. And third, delicts are caused by "humans".[25] Lastly, EDT has numerous stakeholders involved in its production. Attributing liability for damage caused by EDT is a mammoth task that requires costly expert evidence.

These uncertainties have led authors to debate if another legal personality should be created — electronic personalities. Authors who see no need for a new legal personality indicate that the plaintiff in civil delictual[26] claims due to EDT-related damages should determine who in the production line is at fault, thus rooting for product liability.[27] However, this begs the question of which form of liability should be applied: fault-based or strict liability.

This article explores which form of civil strict liability is most suitable where EDT causes a delict. Also, are the South African civil liability doctrines sufficient to oversee EDT? It will be shown that product liability and vicarious liability fall short in these cases. However, there might be a possible solution under the *actio de pauperie* common law doctrine. This will be

22 Minister Ntshavheni's speech. Likewise, the South African President provided that a call for an EDT for a good approach by the International Telecommunications Union (ITU) has been made, but that it still must be adopted by the member states. At the same time, a difficult balance must be struck between protecting human rights *vis-à-vis* damages and risks on the one hand and hindering beneficial progress by overburdening it with overly cautious measures on the other hand. However, in April 2019, the President of South Africa ordered for the Presidential Commission on the Fourth Industrial Revolution (4IR Commission). The members are instructed to assist the government in determining the advantages presented by the 4IR. To attain these relevant policies, strategies and action plans must be drafted that will position South Africa as a global economic player. This suggests that the government is committed to adopting strategies to encourage innovation. https://www.gov.za/speeches/minister-khumbudzontshavheni-remarks-artificialintelligence-ai-regulationwhile (accessed 04-08-2022). It will be shown in this article para 4 that the current strict liability jurisprudence of South Africa is found wanting. That is product liability and vicarious liability. There might, however, be a possible application of the *actio de pauperie*.

23 Duncan, Bowman, Naidoo *et al. Community Psychology: Analysis, Context and Action* (2018) 105.

24 The concept of *ubuntu* was adapted as an ideology by post-apartheid South Africa during the 1990s as a backdrop to bring about harmony and cooperation among the many racial and ethnic groups in South Africa. The ethical values include respect for others, helpfulness, community, sharing, caring, trust, and unselfishness. Ubuntu gives priority to the well-being of the community as a whole. https://www.newworldencyclopedia.org/entry/Ubuntu_(philosophy) (accessed 10-01-2024).

25 Neethling and Potgieter, *Law of Delict* 8 ed (2020) 27, 28–30 provides that "conduct" may be defined as a voluntary human act or omission, which excludes the harm caused by animals. Further, the defence of automatism (the act was carried out mechanically by the acting human) does not provide clarity on the legal personality of AI, thus rendering it legally liable or not for delicts: "It is accepted that the following conditions may cause a person to act involuntarily in that they render him incapable of controlling his bodily movements: absolute compulsion, sleep, unconsciousness, a fainting fit, an epileptic fit, serious intoxication, a black-out, reflex movements, strong emotional pressure, mental disease, hypnosis, a heart attack, low blood-sugar and the like."

26 *Ibid* 27, provides that a delict may be defined as "the act of a person that in a wrongful and culpable way causes harm to another".

27 There is a strong movement and economic motivation to fully automate certain industries (South African President Cyril Ramaphosa, stated that: "In South Africa, we have witnessed the leapfrog effect of AI and related technologies in economic productivity where it has already been deployed in South Africa's banking sector and auto-manufacturing." However, the economic drive is not the question to be discussed here. It is also not inconceivable that AI may cause harm resonating under criminal law jurisprudence. This article will, however, limit its investigation to that of civil law liabilities, specifically that of strict civil liability.

done by exploring the possibility of creating a new electronic legal entity, examining if product liability under the Consumer Protection Act 68 of 2006 (CPA) or the common law vicarious liability doctrine (and related labour legislation) would possibly apply to EDT. After that, the *actio de pauperie* will be investigated. After explaining the challenges with these strict liability principles in South African jurisprudence, the international developments made by the EU will be analysed and explained. The conclusion is that South Africa needs to turn to the EU and member states' product liability regime for more definite solutions. First, a short explanation of EDT is required.

2 THE CHARACTERISTICS OF AI AND IoT

Artificial Intelligence (a machine's ability to perceive, synthesise, and infer information and perform human cognitive functions) and IoT (connectivity between devices to the internet to upload and extract information) are collectively known as EDT. Emerging digital technology may include AI, IoT, blockchain, big data, cybersecurity, robotics, and virtual reality.[28] It is trite among authors[29] that emerging EDT shows levels of complexity and may fall anywhere on a spectrum due to the interdependency between the different components. Emerging digital technology might comprise the following: i) the tangible parts;[30] ii) the different software components and applications;[31] iii) the data itself; iv) the data services;[32] and v) the connectivity features.[33]

Late in 2021, the Future of Privacy Forum released the white paper "The Spectrum of AI: Companion to the FPF AI Infographic", "to provide additional detail and analysis for use of this Infographic tool as an educational resource for policymakers or regulators".[34] These authors argue that EDT can be positioned on a spectrum, depending on the complexity of its components (or rather the methodology it uses or its intended application).[35] It may initially seem simple to determine where EDT resonates on this spectrum, as the explanation states that EDT ranges between "simple automation" and "autonomous decision-making abilities".[36] Even so, authors on EDT provide that the following features are known of AI and are thus more complex than

28 See digital sk://up.

29 Microsoft "AI at Scale" https://www.microsoft.com/en-us/research/project/ai-at-scale/ (accessed 09-06-2022); Anderson, Rainie and Luchinger, "Artificial Intelligence and the Future of Humans" http://tony-silva.com/eslefl/miscstudent/downloadpagearticles/AIhumanfuture-pew.pdf (accessed 09-06-2022).

30 Sensors, actuators, and hardware.

31 SOCI "The Basic Components and Branches of Artificial Intelligence" https://www.meetsoci.com/resources/knowledge/localized-marketing/branches-of-artificial-intelligence/ (accessed 09-06-2024).

32 Collection, processing, curating, analysing and storage.

33 Iyamu and Sekgweleo "Information Systems and Actor-Network Theory Analysis' 2015 *International Journal of Actor-Network Theory and Technological Innovation* 5, 1–11. 10.4018/jantti.2013070101.

34 Future of Privacy Room, "The Spectrum of Artificial Intelligence – An Infographic Tool" https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool/ (AI Spectrum) (accessed 25-06-2022). See also Reimann, "Liability for Defective Products at the Beginning of the Twenty-first Century: Emergence of a Worldwide Standard" 2003 *Am J Comp L* 751.

35 AI Spectrum. There is not 100 per cent consensus around the labels for the various types of AI. Still, for our purposes, we have adopted the following categories as representing generally accepted terms in common use: symbolic AI, including subsets: expert systems, search, and planning and scheduling; rules-based; robotics; computer sensing; knowledge engineering; natural language processing; and of course, machine learning, including deep learning, neural networks, reinforcement learning, and general adversarial networks (GANs).

36 https://www.insidetechlaw.com/publications/what-is-ai (accessed 25-06-2022). These methodologies, which are categorised as follows, place AI on a spectrum: machine learning, deep learning, supervised learning, unsupervised learning, reinforced learning, expert systems, multi-agent systems, and computational argumentation.

mere arrangement on a spectrum:

(a) One such feature is greater complexity — not only does EDT often come with more components themselves, but the algorithms embedded within these products are also increasingly sophisticated.[37] This is further expounded by the fact that EDT more frequently interacts with external sources of information, other actors, and updates, which amplifies the burden of proving a particular chain of events that involved such EDT. Such complexity leads to greater complexity:

> The more complex emerging digital technologies become, the less those taking advantage of their functions or being exposed to them can comprehend the processes that may have caused harm to themselves or to others.[38]

(b) Unlike in the past, many forms of AI no longer leave the factory gate in a final state but are designed to be continuously updated and thereby altered.[39] It is not inconceivable to think that EDT will become more and more autonomous, excluding human interventions. Advanced robots or devices empowered by EDT will have increased capabilities to interpret the environment, interact with humans, cooperate with other EDT, learn new behaviours, and execute goals autonomously without human intervention and control. The more autonomous systems are, the less they depend on different stakeholders and the more significant their impact on their environment and third parties, rendering the behaviour of EDT challenging to predict. AI is meant to improve and thereby alter itself. This autonomy means that rules designed for human conduct will no longer apply.[40]

(c) Likewise, EDT generates (for example, via sensors) and processes data (for example, through algorithms). The availability and the quality of data are essential for its good functioning. Faulty or corrupted data may render the system prone to malfunctioning. At the same time, this openness increases EDT's vulnerability to hacking and other undue influences on its functionalities. After all, the more AI relies upon communication and interaction with external data, the more likely its interfaces may be purposefully abused. But even if there is no constant exchange of information, a mere singular compromised update can already infiltrate the system and, apart from damaging itself, may cause it to inflict harm upon others. Even if the interaction works satisfactorily and is not compromised by hackers, the increasing dependency on constant data input bears the risk that such information is flawed, triggering inappropriate responses to data, which may result in damage despite no

37 Koch "Liability for Emerging Digital Technologies: An Overview" 2020 *Journal of European Tort Law* 115–136 https://doi.org/10.1515/jetl-2020-0137 (accessed 09-06-2022).

38 Final Report of the NTF Expert Group on Liability and New Technologies – New Technologies Formation "Liability for Artificial Intelligence and Other Emerging Digital Technologies" (2019), in the following "Final Report of the NTF" https://op.europa.eu/en/publication-detail/-/publication/1c5e30be-1197-11ea-8c1f-01aa75ed71a1/language-en 33.

39 Koch *Journal of European Tort Law* 120.

40 *Ibid*.

flaw within the algorithms.[41]

(d) AI is open to software extensions, updates, and patches[42] after being put into circulation. Any change to the system's software may affect the entire system or individual components' behaviour or extend its functionality. The software can be patched, updated, or revised by the system producer, individual system components, or third parties in a way that can affect the safety of the EDT. Updates would usually close safety holes through patches, but new codes also add or remove features that change the risk profile of these technologies.[43] It is not inconceivable to predict that if the consumer does not allow the required updates or neglects to allow updates, it may endanger the algorithms of the EDT.

(e) Then there is the human creating the program and algorithms. Bronfenbrenner's ecological systems theory suggests that humans are exposed to environmental factors, which influence such individual's social development. This framework concerns layers of social relationships: micro-systems (family and friendships); exco-systems (organisations and neighbourhoods); and macro-systems (culture and society). A human exists in a constantly changing context, influenced by changing relationships between the layers. In post-Apartheid South Africa, the principle of *ubuntu* has found great stride. This ideology concerns that, at all times, the individual effectively represents the people from whom they come and, therefore, attempts to behave according to the highest standards and exhibit the virtues their society upholds. It is not inconceivable that these principles are enshrined in a South African EDT software programmer, but it may differ from that of another country's programmer's social systems. Emerging digital technologies, such as facial recognition, for example, are biased, resulting in the infringement of human rights.[44]

(f) The milestones in the evolution of human and artificial intelligence highlight the distinct paths and mechanisms of development in these two domains.[45] In the evolution of human intelligence, key milestones include the development of bipedalism, tool use, language, and symbolic thought. Each milestone represents a significant leap in cognitive and social capabilities, enabling our ancestors to adapt, survive, and thrive in changing environments.[46] This is evident in our progress through the previous industrial revolutions. In contrast,

41 Koch *Journal of European Tort Law* 121.

42 "Software patch" is explained as follows: "Throughout its lifetime, software will run into problems called bugs. A patch is an immediate fix to those problems. A software patch or fix is a quick-repair job for programming designed to resolve functionality issues, improve security, or add new features. IT or end users can often download a patch from the software vendor's website. However, the patch isn't necessarily the best fix for the problem, and the product's developers will often incorporate a more complete remediation when they do the next upgrade or full release of the software." https://www.techtarget.com/searchenterprisedesktop/definition/patch (accessed 10-06-2024).

43 Commission Staff Working Document "Liability for Emerging Digital Technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe" (EU AI working document) EUR-Lex - 52018SC0137 - EN - EUR-Lex https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018SC0137 (accessed 10-06-2024).

44 Jammot "Can we Rid Artificial Intelligence of Bias?" 19 May 2024 *TechXplore* ; Buolamwini "Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers" (MIT Master's Thesis 2017) https://www.media.mit.edu/publications/full-gender-shades-thesis-17/ (accessed 13-06-2024).

45 BlockChain Council "Artificial Intelligence vs Human Intelligence" https://www.blockchain-council.org/ai/difference-between-artificial-intelligence-and-human-intelligence/?gad_source=1&gclid=Cj0KCQjw-uK0BhC0ARIsANQtgGNrAEnO0tWprWXmk7y3y-J4Gjb4ptiAQmX3HLa5NjHrbpBS3V7eBFYaAuAzEALw_wcB (accessed 10-06-2024).

46 *Ibid*.

milestones in EDT development are closely tied to technological advancements and theoretical breakthroughs. The development of machine learning algorithms, the rise of neural networks, and the application of AI in diverse fields such as healthcare, finance, and autonomous vehicles represent significant milestones in AI evolution.[47] These milestones in both human and artificial intelligence highlight the complexity and diversity of intelligence as a concept. While human intelligence evolved because of biological, environmental, and social factors over millions of years, EDT is a product of human ingenuity and technological progress, evolving rapidly over just a few decades.[48]

Given the features listed above, it can be reasonably deduced that EDT and human intelligence are closely related features as the operation of EDT is premised on principles of human intelligence. Also, according to its methodologies on the spectrum, EDT's primary features are the ability to think, comprehend, solve problems, learn, or respond. However, there are differences between human intelligence and EDT when one looks at the milestones in the human and EDT evolutions. Given EDT's spectrum and automatous nature, should South Africa consider expanding its civil (and criminal) jurisprudence by creating a new legal entity, "electronic entities"?[49]

3 LEGAL ENTITIES AND LIABILITY

A legal entity should be understood as one participating in legal relations with rights and obligations *vis-à-vis* other legal entities and tangible or intangible objects.[50] Under South African common law jurisprudence, legal entities fall under legal subjects (natural or juristic persons) or legal objects. The most notable attribute of this topic is that of natural and juristic persons' legal capacity and subjectivity. Legal capacity refers to the capability, as prescribed by objective law (*naturalia*), of an entity to have, acquire or dispose of, and enforce rights and duties, and to be held accountable for crimes and delicts.[51] Legal subjectivity refers to being a holder of rights and duties limited by legal capacity as awarded by subjective law.[52]

Therefore, legal entities such as humans and juristic persons have legal capacities (rights and duties). Determining whether EDT can be a legal entity requires referencing its ability to obtain legal capacity.

3 1 Emerging Digital Technology as a Legal Entity

It is assumed, conceivably, that humans are natural legal entities by their very nature — biological properties, social skills, and individual characteristics distinguish them. Therefore, a human is a person, a someone, not a "thing" or an "it".[53] Thus, human legal capacity and dignity

47 *Ibid*.

48 *Ibid*.

49 Nemeiksis "Artificial Intelligence as a Legal Entity in the Civil Liability Context" 2021 *Acta Prosperitatis* 89 https://www.turiba.lv/storage/files/ap-12-makets-rgb.pdf#page=90 93–96; Cerka, Grigiene and Sirbkyte "Is it Possible to Grant Legal Personality to Artificial Intelligence Software Systems?" 2017 *Computer Law & Security Review* 685–699 .

50 Heaton *The South African Law of Persons* 5 ed (2018) 3.

51 Heaton *South African Law of Persons* 35 indicates that the most common capacities are legal capacity (to have rights and duties), capacity to act (to perform juristic acts, therefore acquiring or disposing of rights and duties), and capacity to litigate (to enforce rights and duties).

52 Heaton *South African Law of Persons* 35, provides that these are the rights a legal entity, such as a human or juristic person, has over an object.

53 BlockChain Council "AI".

are assumed to be inherent features.[54] This was, however, not always the case in South Africa.

During South Africa's past, before the era of democracy, slaves were denied legal capacity under Roman and Roman-Dutch law by way of slaves being classified as legal objects, or rather, property of the employer or owner of the slave.[55] Thankfully, this has changed, and "everyone" has the right to dignity, equality[56] and freedom under the democratically guaranteed Constitutional dispensation.[57] Thus, each human has a legal capacity because they are human. Legal capacity is conferred upon humans if they are born alive.[58] Statutes and applicable common law principles confer on humans the legal capacity and, consequently, their status as legal entities.[59]

Ascribing legal personality to EDT does not seem possible.[60] However, there are authors[61] who advocate that EDT's automotive capabilities justify creating a new legal entity, which they call "electronic entities".

One such author is Giedrius Nemeiksis. In 2021, Nemeiksis argued that AI should have legal status as an "electronic entity". This is based on the premise that, due to AI's autonomous nature, and depending on where it lies on the spectrum, it might well be that AI has or will have intellect akin to that of natural entities and, as such, will have to be awarded rights and duties. By referring to the European Parliament in its resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics 2015/2103(INL), this

54 The Constitution of the Republic of South Africa, 1996 (the Constitution) s 10, states, "Everyone has inherent dignity and the right to have their dignity respected and protected".

55 South African History Online "History of Slavery and Early Colonization in South Africa" https://www.sahistory.org.za/article/history-slavery-and-early-colonisation-south-africa (accessed 16-07-2024).

56 The Constitution, s 9, upholds the principle of equality, stating, "Everyone is equal before the law and has the right to equal protection and benefit of the law."

57 The Constitution's Preamble confirms "everyone's" rights: "This Bill of Rights is a cornerstone of democracy in South Africa. It enshrines the rights of all people in our country and affirms the democratic values of human dignity, equality, and freedom."

58 *Road Accident Fund v Mtati* [2005] 3 All SA 340 (SCA) para 7.

59 Examples are the Labour Relations Act 66 of 1995, the Children's Act 38 of 2005, the CPA, the Occupational Health and Safety Act 85 of 1993, and the Unemployment Insurance Act 63 of 2001.

60 Resolution No. 196 of the Council of Ministers on establishing "A policy for the development of artificial intelligence in Poland till 2020" Monitor Polski 2021, item 23.

61 Bayern "The Implication of Modern Business-Entity Law for the Regulation of Autonomous Systems" 2015 *Stanford Technology Law Review* 93–112; Bayern *et al*. "Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators" 2017 *Hastings Science and Technology Law Journal* 135–161; Cerka *et al. Computer Law & Security Review*.

author stated:

> [which] states that today's robots can perform actions that only humans perform normally and exclusively, as well as the development of certain autonomous and cognitive qualities (such as the ability to learn and experience and make decisions almost independently) is increasingly turning them into entities that interact with the environment and can change it.[62]

In support of granting EDT legal personality, authors suggest aspects[63] such as requiring EDT to be registered akin to juristic persons, having insurance or at least the stakeholders involved in its supply and value chain,[64] and having separate legislation regulating EDT.

This was also suggested in the EU Resolution of 2017, which called on the EU

> to explore, analyse and consider the implications of all possible legal solutions, such as: … (f) creating a specific legal status for robots in the long run, so that at least the most sophisticated autonomous robots could be established as having the status of electronic persons responsible for making good any damage they may cause, and possibly applying electronic personality to cases where robots make autonomous decisions or otherwise interact with third parties independently; …[65]

However, this suggestion was criticised and rejected by academics and practitioners as well as the Expert Group on Liability and New Technologies — New Technologies Formation (the Expert Group).[66]

Therefore, this argument on EDT's status as a legal entity seems to gain importance only if its application may lead to an easier assignment of liability for EDT's actions.[67] However, the concept of this status should be akin to the status of legal persons whose actions humans are

62 Nemeiksis *Acta Prosperitatis*.

63 To give a few examples, the following solutions have notably been put forward: (1) the creation of regulatory rules regarding coding and design of robots and autonomous products: Rachum-Twaig "Whose Robot is it Anyway?: Liability for Artificial Intelligence-Based Robots" 2020 *University of Illinois LR* 2020 (4) 1141 -1176 at 1668; (2) establishing a system where the AI would need to be licensed: Kingston "Artificial Intelligence and Legal Liability" Conference Paper, November 2016 https://www.researchgate.net/publication/309695295_Artificial_Intelligence_and_Legal_Liability (citing others) (3) developing a system where AI developers and manufacturers would agree to adhere to certain ethical guidelines to govern AI, providing a framework that courts could use to resolve legal claims where AI is implicated: Allianz Global Corporate and Speciality's website provides for the AGCS Risk Barometer series which frequently publishes on the topics of AI regulation https://www.agcs.allianz.com (accessed 15-06-2022); (4) establishing a regulatory authority dedicated to regulating and governing the development of AI: Scherer "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" 2016 *Harvard Journal of Law & Technology* 353–400, 393–397.

64 EU AI working document n 55 provides that actors in the value chain may include producers, service operators, software providers, traders, conformity assessment bodies and infrastructure providers.

65 European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (n 29), para 59(f). Early draft (version 08.02.2020), submitted as a book chapter: D'Agostino, Piovesan and Gaon (ed) "Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law" (2020) 11. Key questions, however, remain to be settled before concretising this idea. Contrary to corporations, AI would not necessarily have a patrimony of its own and would thus be unable to indemnify its potential victims even if it is found liable. This could, however, be circumvented if some form of compulsory insurance scheme for human stakeholders involved with AI (either designers, manufacturers, service providers, and/or end users) or a compensation fund were to be established simultaneously. In-depth analyses and reflections would also be required to cover the other consequences of granting legal personality to AI, such as the implications concerning its potential criminal responsibility. This suggested solution is also criticised by many. Following the European Parliament's proposal, more than 250 experts from various AI-related fields signed an open letter in 2018 calling upon the European Commission to reject it as it would be — in their opinion — inappropriate, ideological, nonsensical and non-pragmatic.

66 Open letter to the European Commission: Artificial Intelligence and Robotics (Open letter: AI) http://www.robotics-openletter.eu/ (accessed 14-06-2022).

67 Ziemianin "Civil Legal Personality of Artificial Intelligence: Future or Utopia?" 2021 *Internet Policy Review* https://doi.org/10.14763/2021.2.1544

liable for, not to the concept of natural persons who bear liability themselves.

However, legal jurisprudence is premised on principles of morality and human values, which emphasise humanity and dignity.[68] Human dignity results from this humanity, which includes living birth and creating social structures.[69] In civil law, legal capacity is understood as the possibility of acquiring rights and obligations resulting from such dignity.[70]

Humans create emerging digital technologies to perform specific tasks. Therefore, it cannot be said that digital technology has inherent biological properties or social attributes of its own accord. Even if these properties can be attributed to it, or EDT may be subjected to specific social processes, EDT is programmed by its creator: a human. By the nature of EDT, it is impossible to speak of its "live birth". Although EDT can imitate humans, it cannot be assumed that it is a natural legal entity. Hence, EDT can only be normative: derived from and established by the provisions of the law. Thus, EDT is not a natural entity with rights and duties akin to a human legal person.

To date, EDT has no legal status or personality, thus no rights or duties. This does not mean that countries will consider creating electronic entities to regulate autonomous EDT in the future, thereby ascribing rights and responsibilities to it. For now, one cannot sue EDT for delictual damages caused by itself. This is the position in the EU and South Africa. As such, what follows is to determine if the current doctrine of strict liability in South Africa is suitable for matters concerning delictual damages caused by EDT.

4 SOUTH AFRICAN DELICTUAL LIABILITY: PRODUCT, VICARIOUS AND ACTIO DE PAUPERIE

4 1 Background

Delictual liability is the general liability doctrine applicable to a wrongful act or omission committed by one person towards another, causing damage.[71] A delict is based on fault and assigns liability to the legal subject (natural or juridical persons) responsible for failing to take reasonable care to avoid injury or loss to another.[72] Assigning liability depends on which form of liability would find application: fault liability or strict liability. Fault liability concerns that victims are strictly liable for their losses unless the injurer is at fault.[73] On the other hand, strict liability concerns that injurers are strictly liable for the losses they incur unless the victim is at fault.[74]

Under strict liability, the element of fault need not be shown, as opposed to fault liability. Under the common law strict liability doctrine, one would find product liability,[75] vicarious liability[76]

68 Steinmann "The Core Meaning of Human Dignity" 2016 *PELJ* http://dx.doi.org/10.17159/1727-3781/2016/v19i0a1244

69 *Ibid*.

70 It is different in the case of other entities upon which provisions of civil law currently confer the status of a legal entity: juristic persons. Their status as legal entities is regulated by statutes such as the Companies Act 71 of 2008 (Companies Act). The aim is to provide for the incorporation, registration, organisation, and management of companies, the capitalisation of profit companies, and the registration of offices of foreign companies carrying on business within the Republic. See also Ziemianin *Internet Policy Review*.

71 Neethling *et al. Law of Delict* 6 ed (2010) 355.

72 Neethling and Potgieter *Law of Delict* 4.

73 Neethling et al. *Law of Delict (2010)* 329.

74 Neethling and Potgieter *Law of Delict* 386 and 456.

75 *Ibid* 382–386. See also Koziol *Product Liability: Conclusions from a Comparative Perspective* (201) 532–534.

76 Neethling and Potgieter *Law of Delict* 444–454; *Stein v Rising Tide Productions CC* 2002 5 SA 199 (C) 205.

and the *actio de pauperie*.[77] A few South African statutes replicate strict liability as a common law doctrine. The CPA is one such example,[78] and it has, to date, found application in defective product liability claims.[79]

4 2 Statutory Product Liability: Consumer Protection Act 68 of 2006

Product liability is a form of statutory extra-contractual liability referring to the civil liability of stakeholders involved in the production and supply chain of products or goods.[80] Product liability generally applies to manufacturers of finished products and raw parts or components included in a finished product.[81] It may also apply to importers, designers, distributors, suppliers and retailers of the product.[82] Product liability may concern (1) manufacturing defects, (2) design defects, and (3) failure to warn users against the product's inherent, non-obvious dangers.[83]

In the past, product liability was problematic as it resonated under the (fault-based liability) *Aquilian* action;[84] all the elements of a delict had to be shown to award the plaintiff compensation.[85] Fault was notoriously difficult to prove; either negligence or intent of the manufacturer had to be shown. Thus, the plaintiff needed to show, by using expert evidence, that the delict is due to the fault of one, some or all of the stakeholders in its production and supply chain.[86] This then put the plaintiff in an unjustifiably undermining position compared to the producer or manufacturer. This was due to the information required as evidence: it is expensive and time-consuming, and more often than not, the manufacturer does not want to provide any information due to

77 Neethling and Potgieter *Law of Delict* 307, 435–438.

78 Bourie, Fagan *et al*. "Product Liability in the Rest of the World" in Koziol *et al*. (eds) *Product Liability: Fundamental Questions in a Comparative Perspective* (2018) 464–494 https://doi.org/10.1515/9783110547559-022

79 Neethling and Potgieter *Law of Delict* 456–458.

80 Barnard "An Overview of the Consumer Safety and Product Liability Regime in South Africa" 2021 *IJCLP* 25.

81 Gowar "Product Liability: A Changing Playing Field?" 2011 *Obiter* 521.

82 Van Heerden and Barnard "Narrowing the Reach of the Strict Product Liability Provisions in Section 61 of the Consumer Protection Act 68 of 2008 in View of *Eskom Holdings Ltd v Halstead-Cleak* 2017 1 SA 333 (SCA)" 2019 *THRHR* 444.

83 Basson "The South African Law on Product Liability – Quo Vadis" 2011 *South Afr J Ind Eng* 83–99.

84 Gowar *Obiter* 522. Corbett "Extending the Reach of Justice: The Role of the Aquilian Action in South African Law" 1998 *N. Ir. Legal Q* 23.

85 Van Eden and Van Wyk "Product Liability in South Africa" 1998 *26 Int'l Bus. Law* 63.

86 Neethling, Potgieter and Visser state that the principles found in Anglo-American law should be followed, being the doctrine of *res ipsa lioquitur* (the facts speak for themselves) (Neethling *et al*. *Law of Delict* (2010) 385).

intellectual property rights.

As such, the CPA was enacted, protecting "consumers"[87] with section 61 regulating product liability. This section holds the producer[88] or importer,[89] distributor[90] or retailer[91] of any goods liable for any harm caused wholly or partly as a consequence of supplying any unsafe goods;[92] a product failure, defect or hazard in any goods; or (c) inadequate instructions or warnings provided to the consumer of any risk arising from or associated with the use of any goods, irrespective of whether the harm resulted from any negligence on the part of the producer, importer, distributor or retailer.[93]

Thus, the CPA imposes strict liability on manufacturers, producers and sellers for harm caused by defective[94] products. These stakeholders may be held liable for damages even if they were not negligent or did not intend to cause harm. The plaintiff must prove on a balance of probabilities the damage, the defect and the causal link between the defect and damage;[95] however, no proof of negligence is required.[96] Once this burden of proof is fulfilled, the stakeholder must provide

87 The CPA affects a wide range of consumers and transactions. The definition of a "consumer" includes not only the person (either a natural or juristic person) to whom goods or services are promoted or supplied but also the actual user of the goods or the recipients or beneficiaries of the services. In other words, a consumer may be someone other than someone who entered into an agreement with a supplier and paid for the goods or services. In practice, this would mean that if you are given a spa treatment as a birthday present, you will be entitled to the consumer protection measures in the Act, even though you never agreed with the spa.

88 The CPA, s 1 defines "producer" as "a person who — (a) grows, nurtures, harvests, mines, generates, refines, creates, manufactures or otherwise produces the goods within the Republic, or causes any of those things to be done, with the intention of making them available for supply in the ordinary course of business; or (b) by applying a personal or business name, trade mark, trade description or other visual representation on or in relation to the goods, has created or established a reasonable expectation that the person is a person contemplated in paragraph (a)."

89 The CPA, s 1 defines an "importer", concerning any particular goods, to mean "a person who brings those goods, or causes them to be brought, from outside the Republic into the Republic, with the intention of making them available for supply in the ordinary course of business".

90 The CPA, s 1 defines "distributor", to any particular goods, means "a person who, in the ordinary course of business — (a) is supplied with those goods by a producer, importer or other distributor; and (b) in turn, supplies those goods to either another distributor or to a retailer".

91 The CPA, s 1 defines "retailer", for any particular goods, to mean "a person who, in the ordinary course of business, supplies those goods to a consumer".

92 The CPA, s 1 provides that "goods" include — "(a) anything marketed for human consumption; (b) any tangible object not otherwise contemplated in paragraph (a), including any medium on which anything is or may be written or encoded; (c) any literature, music, photograph, motion picture, game, information, data, software, code or other intangible product written or encoded on any medium, or a licence to use any such intangible product; (d) a legal interest in land or any other immovable property, other than an interest that falls within the definition of 'service' in this section; and (e) gas, water and electricity".

93 Gowar *Obiter* 522.

94 The CPA, s 53 defines "defect". In short, it means any material imperfection in the manufacture of the goods or components, or the performance of the services, that renders the goods or results of the services less acceptable than persons are generally reasonably entitled to expect in the circumstances, or any characteristic of the goods or components that renders the goods or components less useful, practicable or safe than persons are generally reasonably entitled to expect.

95 The only damages that can be recovered due to harm caused by defective or unsafe products are actual, proven damages in South Africa. Where damages are awarded for pain and suffering resulting from bodily injuries, they must be proved regarding common law judgments relating to similar injuries. Punitive damages are not available under South African law under any circumstances. Neethling and Potgieter *Law of Delict* (2010) 385.

96 To establish liability under the CPA, a party will have to prove that harm was caused, wholly or partly, as a consequence of: "The supply of an unsafe product, a product failure, defect or hazard in the product, inadequate instructions or warnings provided to the consumer pertaining to any hazard arising from, or associated with, the use of the product," See s 53 of the CPA.

compensation regardless of negligence or fault.[97] Manufacturers can rebut liability under certain conditions unrelated to fault or negligence considerations.[98] These defences include the state of scientific or technical knowledge when the product was put into circulation,[99] which could not allow manufacturers to detect the defect or that no defect existed when the product left their hands.[100]

It should be noted that the CPA applies to an agreement between a consumer and a supplier in the ordinary course of business.[101] A consumer buys from the supplier, the person or company that sells goods, renders services, and/or advertises its goods or services to the consumer. The concern is that a party who did not directly purchase from the supplier will not find protection under section 61 of the CPA. This also does not include innocent bystanders who are not users, beneficiaries or recipients, injured by a defective product will still need to rely on the ordinary delictual principles of common law.[102]

It should also be noted that the CPA does not define "product" but does contain a definition for "goods". The only mention close to EDT in this definition includes "… information, data, software, code or other intangible product written or encoded on any medium …".[103] This thus excludes services such as software updates required for EDT safety.[104]

The CPA, however, contains exclusions,[105] in which case, the plaintiff must rely on the general common law principles of delict (that is, fault-based liability). Section 5(2) provides that this Act does not apply to any transaction in terms of which goods or services are promoted or supplied to the state, where the consumer is a juristic person whose asset value or annual turnover, at

97 Liability can be joint and several. Liability will be apportioned based on the percentage of negligence or contributory negligence found by the South African court. No order will be made against a person or entity not joined to the proceedings. Stakeholders are usually advised to obtain insurance for such cases. See Katzew and Mushariwa "Product Liability Insurance in the wake of the Consumer Protection Act 68 of 2008" 2012 *SA Merc LJ* 1–15.

98 Gowar *Obiter* 523. See also Buys *Selected Aspects Relating to Defenses to Strict Product Liability as Introduced by the Consumer Protection Act of 68 of 2008* (Master's thesis, University of Pretoria 2016).

99 Machnikowski *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies* (2016).

100 Under South African law, claims must be brought within three years. Liability will not arise where (s 61(4), CPA): "The unsafe product characteristic, failure, defect or hazard that results in harm is wholly attributable to compliance with any public regulation; the alleged unsafe product characteristic, failure, defect or hazard: did not exist in the goods at the time a person supplied it to another person alleged to be liable; or was wholly attributable to compliance by that person with instructions provided by the person who supplied the goods to that person, in which case the point above does not apply. It would be unreasonable to expect the distributor or retailer to have discovered the unsafe product characteristic, failure, defect, or hazard with regard to that person's role in marketing the goods to consumers."

101 The CPA, s 1 defines "consumer".

102 Neethling and Potgieter *Law of Delict* (2010) 374.

103 The CPA, s 1.

104 Alheit "The Applicability of the EU Product Liability Directive to Software" 2001 *CILSA* 188–209; Kriek *The Scope of Liability for Product Defects under the South African Consumer Protection Act 68 of 2008 and Common Law – A Comparative Analysis* (Doctoral dissertation, Stellenbosch University 2017).

105 One such exemption is that of no nexus between the plaintiff and the respondent. This is illustrated in *AB Ventures Ltd v Siemens Ltd* 2011 4 SA 614 (SCA), where the appellant concluded a written agreement with Lumwana Mining Company Limited, under which the appellant undertook to construct and complete the Lumwana Copper Mine in northern Zambia. Several parties were involved in the supply chain. The respondent had to supply four specialised electrical units, all of which turned out to be defective. The appellant unsuccessfully sued the respondent for damages, and the court concluded that there was no legal nexus between the appellant and the respondent. Therefore, there must be a nexus between the plaintiff and respondent, setting out the ambit of their reciprocal rights and duties. While the nexus persists, each party has adequate remedies if the other commits a breach. Damages for product defects, thus, that fall outside the ambit of the CPA, would not extend to a plaintiff "not in contractual privity", for example. Another example of a nexus may be a warranty.

the time of the transaction, equals or exceeds the threshold value determined by the Minister,[106] if the transaction falls within an exemption granted by the Minister. This constitutes a credit agreement under the National Credit Act (but the goods or services that are the subject of the credit agreement are not excluded from the ambit of the CPA), giving effect to a collective bargaining agreement within the meaning of section 23 of Constitution of the Republic of South Africa, 1996 (the Constitution) and section 213 of the Labour Relations Act (the LRA),[107] or about services to be supplied under an employment contract.

The reason for the last-mentioned exclusion in section 5(2) (employment contracts) is due to the regulation provided for by the LRA, the Occupational Health and Safety Act[108] (OHSA), the Employment Equity Act[109] (EEA) and the Basic Conditions of Employment Act[110] (BCEA). These statutes provide for the employer's statutory obligations to *inter alia* prevent risk, as far as reasonably possible, in the workplace *vis-à-vis* employees and third parties. In addition, should an employee cause a delict within the course and scope of employment, the employer may be found liable on the principles of the common law vicarious liability doctrine.[111] These statutes and the common law doctrine concern strict liability. The concern is that these statutes and common law doctrine encompass delictual acts committed by "humans" or "a person" and not EDT. This will be analysed hereafter.

To conclude, irrespective that the plaintiff does not have to prove fault, to determine who in the production line of EDT might be sued (due to the complexities of EDT), the exclusions limiting the CPA's application is expensive and time-consuming for the plaintiff to gather expert evidence, and to present to a court who might not have EDT expertise, the section 61 CPA product liability regulation falls short of a justifiable claim. This deters plaintiffs from pursuing legal recourse.

4 3 Delictual Liability within the Workplace

4 3 1 Introduction

It is trite that the preceding industrial revolutions demanded that most legal systems evolve. The traditional employment relationship, as it was known during the prior industrial revolutions, with predominant human interaction, is, in certain instances, altered by the introduction of EDT in the current 4IR.[112]

The South African legal system, guided by the principles enshrined in the Constitution, is commanded to adapt the protection provided to society.[113] This has brought about, and still does, substantial changes in various branches of South African law, including workplace-related law.[114]

As a result, the South African employment sphere has been converted to meet society's national and international requirements and protect employees from various risks. These risks include

106 Currently, the asset value or annual turnover exceeds two million rand.

107 66 of 1995.

108 85 of 1993.

109 55 of 1998.

110 75 of 1997.

111 See discussion of vicarious liability at para 4 3 of this article.

112 Webster and Ivanov "Robotics, Artificial Intelligence, and the Evolving Nature of Work" in George and Paul (eds) *Digital Transformation in Business and Society* (2020) https://doi.org/10.1007/978-3-030-08277-2_8

113 The Constitution, s 2 reads: "This Constitution is the supreme law of the Republic; law or conduct inconsistent with it is invalid, and the obligations imposed by it must be fulfilled."

114 Labour-related legislation which refers to the worker as "an employee" will need to be amended to allow for regulation of AI.

employment injury and harm caused by third parties.[115] The Constitution prescribes various fundamental rights that advance labour protection. This extends to parties to work relationships and not only those in traditional/formal employment relationships. This is evident from the wording used in section 23. To give effect to these fundamental rights, subsequent labour legislation such as the LRA, the OHSA, EEA, and the BCEA, has provided guidelines and protection to the parties in the employment relationship. Should a person, for being excluded from the ambit of the said legislation, need to claim damages for a delict, they need to turn to the common law doctrine of vicarious liability.[116] However, the exact parameters of what or who an "employee" may be is still the topic of much debate.

4 3 2 Revisiting the Definition of an "Employee"

The current definition of an "employee" has a long history. The common law in South Africa is inherited from the Roman and Roman-Dutch systems in which the definition of an "employee" is premised on a contract of employment.[117] In dispute cases, the presiding officer examined the employment contract regarding letting and hiring between a "master and servant".[118] Here, the master's supervision and control over the servant's services delivered was analysed to determine whether the person was an "employee". This was the introduction of the common law control test. The control test, however, proved insufficient as an employment relationship became rebuttable akin to that of independent contractors and agencies. Subsequent common law tests were developed to determine the exact parameters of an "employee". These were the organisational, economic dependency and, finally, the dominant impression test.

After these common law tests, the statutory employment relationship emerged, as seen in the Transvaal Industrial Disputes Prevention Act[119] in which an "employee" was defined to mean "any white person engaged by an employer to perform, for hire or reward, manual, clerical, or supervision work in any undertaking, trade, or industry to which this Act applies … ". Then, the Industrial Conciliation Act,[120] which again excluded non-white citizens from the definition of an "employee", which was amended by the Industrial Conciliation (Amendment) Act,[121] followed

115 See, for example, the Preamble of the Occupational Health and Safety Act 85 of 1993 (the OHSA): The primary aim of the OHSA is to "provide for the health and safety of persons at work and for the health and safety of persons in connection with the use of plant and machinery; the protection of persons other than persons at work against hazards to health and safety arising out of or in connection with activities of persons at work; to establish an advisory council for occupational health and safety; and to provide for matters connected therewith." And s 4 of the OHSA which provides for employers' duties and responsibilities to protect the safety and health of workers and others.

116 Botha and Millard "The Past, Present and Future of Vicarious Liability in South Africa" *De Jure* 2012. https://hdl.handle.net/10520/EJC135279 (accessed 15-06-2022).

117 Schaeffer *Industrial Law (Including Law of Master and Servant)* (1965) 363.

118 Barlow *The South African Law of Vicarious Liability in Delict and a Comparison of the Principles of other Legal Systems* (LLD thesis, University of Stellenbosch 1994); Madhuku "Vicarious Liability of an Employer for the Delictual Acts of his Servant under Zimbabwean Law" 2009 *Journal of African Law* 181–188. "Master's Liability to Third Person: Recovery from Servant" (1957) *SALJ* 226.

119 20 of 1909.

120 11 of 1924.

121 24 of 1930.

by a further Amendment Act[122] and was repealed by the Industrial Conciliation Act.[123] The Industrial Conciliation Act of 1956 then empowered the Minister of Labour to implement job reservation, which meant that only a specific group could be "employees",[124] rendering certain groups still excluded as "employees" with labour-related rights and protection. This might have served the economically powerful employer; however, it was also to its detriment: making use of labour that fell outside the scope of what was defined as an "employee" meant they could not dismiss as a form of recourse for misconduct, or delicts caused by the one who rendered service in its name. Thus, vicarious liability could not be applied. The Labour Relations Act then repealed the Industrial Conciliation Act[125] (LRA of 1956).

A dispensation followed in the LRA of 1956. Here, "employee" was defined to mean

> any person (other than Buntu) employed by, or working for any employer and receiving, or being entitled to receive any remuneration, and receiving, or being entitled to receive any remuneration, and any other person whatsoever (other than Buntu) who in any manner assists in the carrying on or conducting of the business of an employer …[126]

This definition was amended as the government at the time accepted non-white persons as employees.[127] Section 1(a) of the Labour Relations Amendment Act[128] defined "employee" to mean

> any person who is employed by or working for an employer and receiving or is entitled to receive any remuneration and, subject to subsection (3), any person whomsoever who in any manner assists in the carrying on or conducting of the business of the employer …

A similar definition was also added to the Basic Conditions of Employment Act of 1983,[129] which was replaced by the BCEA.

With the enactment of the democratic Constitution, previous legislation that did not provide equality, dignity, and freedom had to be either amended or repealed completely. As such, the LRA, BCEA, and all other applicable legislation had to be amended or implemented, as in the case of the EEA. Section 213 of the LRA now defines an "employee" as a person who includes

122 7 of 1933.

123 36 of 1937. In Act 36 of 1937 "employee" was defined to mean "any person employed by, or working for any employer, and receiving, or being entitled to receive, any remuneration, and any other person whatsoever who in any manner assists in the carrying on or conducting of the business of an employer but does not include a person, whose contract of service or labour is regulated by Act 40 of 1984 of Natal, or, in terms of s 2 of the Masters and Servants Law (Transvaal and Natal) Amendment Act, 1926 (Act 26 of 1926), is regarded for the purpose of Act No. 40 of 1984 of Natal as a contract between master and servant, or is regulated by the Native Labour Regulation Act, 1911 (Act 15 of 1911), or by the Natives (Urban Areas) Act, 1923 (Act 21 of 1923), or by any amendment of, or any regulation made under, any of those laws; and 'employed' and 'employment' have corresponding meanings…"

124 The Industrial Conciliation Act of 1956, s 24: "employee" means "any person engaged by an employer to perform, for hire or reward, manual, clerical or supervision work in any undertaking, industry, trade or occupation to which this Act applies, but shall not include a person whose contract of service or labour is regulated by any Native Pass Laws and Regulations, or by Act 15 of 1911 or any amendment thereof or any regulations made thereunder, or by Law 25 of 1891 of Natal or any amendment thereof, or any regulations made thereunder, or by Act 40 of 1894 of Natal or any amendment thereof …"

125 28 of 1956.

126 *Wyeth SA (Pty) Ltd v Manqele* (2005) 26 ILJ 749 (LAC).

127 See s 1(c) of Act 94 of 1979, as amended by s 1(f) of Act 57 of 1981 and by s 1(a) of Act 2 of 1983.

128 Act 2 of 1983.

129 3 of 1983.

(except independent contractors) all irrespective of their race:

> (a) any person, excluding an independent contractor, who works for another person or for the State and who receives, or is entitled to receive, any remuneration;
>
> b) any other person who in any manner assists in carrying on or conducting the business of an employer, …

The EEA and the Skills Development Act[130] contain the exact definition of "employee", referring to a "person", not EDT, as an employee. Therefore, the historical development of what constitutes an "employee" in South Africa resonated around concerns about race and not about whether EDT should also be included.

4 3 3 Statutory Exclusions

In addition to the above concern regarding who is an employee, employment legislation contains exclusions. Overall, these statutes exclude independent contractors from its ambit. The LRA excludes, for example, the National Defence Force and the State Security Agency.[131] Another example can be found in section 3 of the BCEA: members of the State Security Agency, unpaid volunteers working for an organisation serving a charitable purpose, and persons employed on vessels at sea. This means then that a plaintiff will resort to the constitutional right to fair labour practices[132] and the common law principle of vicarious liability. However, as indicated above, the vicarious liability doctrine only applies to humans, not EDT.

4 3 4 Concerns with Vicarious Liability

These exact parameters of what an "employee" is are significant to this topic as a delict caused by an "employee" during the course and scope of employment provides remedies to a plaintiff under the auspices of the extra-contractual[133] vicarious liability doctrine.[134] This doctrine to date has been applied where employees, as human legal entities, commit delicts. This excludes delicts caused by independent contractors. However, given the inevitability which prevails during the current 4IR and EDT, the doctrine of vicarious liability gains more significant importance in a context where EDT engages with human beings or where humans program EDT to perform specific tasks and delicts ensue.[135]

Several theories justify the doctrine that an employer may be held liable for the delicts caused by its employee during the course and scope of employment without fault to the employer.[136] The risk theory turns on the premise that where an employee's activities create a considerable

130 97 of 1999.

131 LRA, s 2.

132 Constitution, s 23.

133 Extra-contractual liability relates to civil law responsibility for damage caused outside the context of a contract (the damage being caused by a violation of a right or legitimate interest protected by law). It can be imposed by general civil law rules or specific legislation.

134 Neethling *et al. Law of Delict* (2010) 365.

135 Etsebeth "The Growing Expansion of Vicarious Liability in the Information Age (Part 1)" 2006 *TSAR* 564–580. Etsebeth "The Growing Expansion of Vicarious Liability in the Information Age (Part 2)" 2006 *TSAR* 752–765. Midgley "Mandate, Agency and Vicarious Liability: Conflicting Principles" 1991 *SALJ* 419.

136 Botha and Millard *De Jure* 227. See also Nana "Sexual Harassment in the Workplace in South Africa: The Unlimited Vicarious Liability of Employers?" 2008 *JAL* 245–267. Scott "The Theory of Risk Liability and its Application to Vicarious Liability" 1979 *CILSA* 44–64. Wagener "The Relationship(s) Giving Rise to Vicarious Liability in South African Law" 2014 *SALJ* 178–204.

risk of causing a delict, there is sufficient justification for holding the employer liable.[137] Scott[138] indicates that the risk theory should be the foundation of the doctrine of vicarious liability. Where instructions are given to employees, certain risks may safely be assumed to be possible, and wrongful acts may be committed. For this, the employer should be held liable due to the risk an employer takes when employing that specific person out of all the applicants for that vacancy.[139]

The prime focus of holding the employer liable seems to be on that employer: it is in that employer's interest to outsource what it should (or wants to) have done to another (the employee), and, therefore, it should bear the consequences.[140] Also, the employee's conduct is evaluated according to standards applicable to the employer, as the employee merely steps into the employer's shoes for the employer's profit (so-called "subrogation principle").[141] If EDT instead harms a third party while being used for (or even by) the employer, this should not make a difference … or should it?

However, even though the principle of subrogation seems to dictate such a conclusion, it cannot eliminate a fundamental problem inherent in that reasoning: How can the operation of an AI-driven machine be measured according to standards that apply to human conduct? In South Africa, strict liability resonates on the premise that the employer has control over and benefits from using the "employee" (who is, to date, a human). Whether in writing or not, an agreement was made between the employer and the human employee. This agreement is not present when an employer uses EDT — an employer disagrees with the EDT on what it should do to ultimately make a profit for the employer. Instead, it is an agreement between the employer and the manufacturer, the producer and or the supplier on what the EDT should do to achieve the employer's goals.

Therefore, similarly to the section 61 CPA product liability regulation, vicarious liability cannot be applied in EDT delicts. Humans might create emerging digital technology, but it does not resonate with the definition of an "employee". For now, an employer should be sued under the auspices of the OHSA, the LRA, EEA, or BCEA, as the case may be.[142] However, this is only sometimes suitable, as these statutes contain exclusions. In such a case, the plaintiff

137 Neethling "Risk-creation and the Vicarious Liability of Employers" 2007 *THRHR* 527.

138 Scott *Middellike Aanspreeklikheid in die Suid-Afrikaanse Reg* (1983) 390–391. Manamela "Vicarious Liability: Paying for the Sins of Others: Case Comments" 2004 *SA Merc LJ* 125–132.

139 In *Feldman (Pty) Ltd v Mall* 1945 AD 733 738 the court referred to *culpa in eligendo* (fault in the choice of an employee). Therefore, the employer has an irrefutable presumption that the master has been negligent if his servant commits a delict. See Neethling and Potgieter *Law of Delict* (2010) 445 vn 122.

140 Calitz "Vicarious Liability of Employers: Reconsidering Risk as the Basis for Liability" 2005 *TSAR* 215–235.

141 Subrogation is a principle employed in insurance law. It refers to a person or a group substituting another for damage or debt, accompanied by transferring rights and duties. It can also be applied in the employment context under vicarious liability. See Procaccia, "Vicarious Tort Liability, Employer's Liability Insurance and Subrogation: A Problem of Conflicting Policies" 1972 *Ins LJ* 471

142 Min *et al*. "The Fourth Industrial Revolution and Its Impact on Occupational Health and Safety, Worker's Compensation and Labor Conditions" 2019 *Saf Health Work* 10.1016/j.shaw.2019.09.005 Artificial intelligence is used extensively to create so-called bots, i.e., programs whose purpose is to replace people [Grimme *et al*. *Demystifying Social Bots: On the Intelligence of Automated Social Media Actors* (2017) 279; Klopfenstein *et al*. *The Rise of Bots: A Survey of Conversational Interfaces, Patterns and Paradigms* (2017) 555–565 https://dl.acm.org/doi/10.1145/3064663.3064672]. Bots perform their tasks primarily in the services market, in the absence of human beings. One of the bots tested by IT tools producers for the needs of internet communication was a Microsoft product called "Tay", which interacted with the public via Twitter. The bot created its entries based on interactions with the users of this portal. However, within a few hours of operation, it began to publish offensive entries, so the project was closed (Neff and Nagy "Agency in the Digital Age: Using a Symbiotic Agency to Explain Human-technology Interaction" in Papacharissi (ed) *A Networked Self: Human Augmentics, Artificial Intelligence, Sentience* (2018) 4915.

should resort to the common law vicarious liability doctrine. This is not possible in the cases of exclusions, as vicarious liability applies to humans as employees. Therefore, this is a dead-end circle.

4 4 *Actio de Pauperie*

Another interesting example of strict liability under South African common law is that of liability about damage caused by domestic animals: the *actio de pauperie doctrine.*[143] Although the domestic animal is the cause of the damage, the owner bears sole compensatory responsibility for any such damage.[144] The *actio de pauperie* remains ingrained in South African jurisprudence.[145] As articulated in *Fourie v Naranjo*,[146] there are three requirements for a claim to be successful:

(a) The wrongdoer/defendant must be the owner of the domestic animal when the damage was inflicted.

(b) The animal must be domesticated[147] and must have acted contrary to its nature (*contra naturam sui generis*) when inflicting the damage.[148] This requirement further requires the animal to have caused the damage spontaneously and because of inward vice/excitement (*sponte feritate commota*).[149] The defendant has the onus to prove the following defences to rebut liability: the animal reacted to external stimuli and not due to internal vice; *vis maior*;[150] provocation or culpable conduct on the part of the plaintiff, on the part of a third party, or provocation by another animal;[151] prejudiced party voluntarily assumed risk;[152] or an existing indemnity between themselves and the plaintiff in terms of which the claimant indemnified the defendant against any damage that may arise as a result of the behaviour of the animal.[153]

(c) The victim or prejudiced person or their property must have been lawfully present at the location where the damage was inflicted.[154] The defendant may be absolved of liability if he/she can prove that the plaintiff had no legal right to be on the property as they were, for

143 Loubser "Strict Liability: Private Law and Human Rights: Bringing Rights Home in Scotland and South Africa" (2012) 205–234. Mukheibir "Barking up the Wrong Tree–The *Actio De Pauperie* Revisited: *Van Meyeren v Cloete* (636/2019) [2020] ZASCA 100 (11 September 2020)" 2021 *Obiter* 703–713.

144 Wagner "Dog Owners Beware: Strict Liability for Dog Attacks" 1 February 2017 *De Rebus* https://www.derebus.org.za/dog-owners-beware-strict-liability-dog-attacks/ (accessed 14-05-2024).

145 See *O'Callaghan NO v Chaplin* 1927 AD 310. Polojac "*Actio de pauperie*: Anthropomorphism and Rationalism" 2012 *Fundamina* 119–144.

146 *Fourie v Naranjo and Another* 2008 1 SA 192 (C).

147 A distinction must be maintained between wild animals, presumed to be dangerous or ferocious by nature (*ferae naturae*) and domestic animals, regarded as being tame in nature.

148 This requirement entails adopting an objective stance to determine whether the animal acted contrary to the behaviour that may reasonably be expected of an animal in the applicable genus; see *Loriza Brahman v Dippenaar* 2002 2 SA 477 (SCA) 485.

149 Wagner *De Rebus*.

150 An unforeseeable intervening force of nature.

151 Neethling *et al. Law of Delict* (2010) 358.

152 This is referred to as the defence of *volenti non fit iniuria.* The defence of *volenti non fit iniuria* considers the plaintiff's subjective state of mind to determine whether the danger, which materialised, was apparent to and appreciated by the claimant. See *Santam Insurance Co Ltd v Vorster* 1973 4 SA 764 (A).

153 Refer to the CPA for strict requirements about good quality and safe goods found in ss 53–61.

154 Courts' interpretations of this requirement differ, as some judgments refer to the claimant having a "lawful purpose" while others require a "legal right". There appears to be a preference for the "legal right" approach, as it may be challenging to ascertain the "lawful purpose" of property.

example, an intruder.[155]

For the plaintiff to prove negligence, the plaintiff has the onus to prove the requirements set out in the "reasonable person test", as articulated in *Kruger v Coetzee.*[156] This onus, on a balance of probabilities, entails the plaintiff to prove whether a *diligens paterfamilias* in the position of the defendant would foresee the possibility of his or her conduct causing injury to another or to the property of another and leading to subsequent patrimonial loss; and take reasonable steps to guard against this occurrence.[157]

It is not inconceivable to see EDT, due to its autonomous feature, akin to that of animals and the delictual liability applied to animals under the *actio de pauperie* doctrine. This common law remedy provides that "*the owner of an animal that attacks a person who was lawfully at the place where he was injured, and who neither provoked the attack nor by his negligence contributed to his injury, is liable, as owner, to make good the resulting damage*." The *actio de pauperie* applies where harm is caused by no fault of the animal's owner.[158] Strict liability is thus imposed on the owner of the domestic animal.[159] This doctrine may thus provide guidelines for South Africa to consider regulating EDT liability instead of product and vicarious liability.

5 CHALLENGES AND SHORTCOMINGS OF CURRENT SOUTH AFRICAN LIABILITY PRINCIPLES

Whereas the South African general common law of delict, product liability, and vicarious liability seem to not suggest appropriate answers in "simpler" cases of delicts caused by EDT, their application may be found wanting when it concerns cases implicating the most advanced forms of EDT. Each case should be determined on its own merits and thus has its facts and features that are undoubtedly complex. In cases involving a high number of stakeholders,[160] EDT is becoming increasingly autonomous and tracking its thought processes. It requires data services (collection, processing, curating, analysing, and updating software) and connectivity features.

The designers and programmers set goals for the EDT instead of programming all possible scenarios or giving precise instructions. Emerging technologies process the data input, learn from it, and decide the best course of action to reach its goal. In the long run, the programmers may be unable to pinpoint the stages leading to success; put differently, they cannot explain the EDT's "thought process" leading to obtaining the goal or not. Hence, programmers cannot determine if legal aspects were indeed considered by the EDT as the data fed into the algorithm may be so diverse and ever-changing. It is often impossible to reproduce the surrounding circumstances in which the delict occurred and thus to identify its source.

This ebb and flow ultimately affect the causation required for delictual and product liability claims. On a balance of probabilities, the plaintiff must prove the breach of duty of care and a

155 Scott "Conduct of a Third Party as a Defence against a Claim Based on the *Actio de Pauperie* Rejected-*Cloete v Van Meyeren* [2019] 1 All SA 662 (ECP); 2019 2 SA 490 (ECP)" 2019 *THRHR* 321. Van der Merwe "The Defence of Conduct of a Third Party in View of the Rationale for Strict Liability in Terms of the Pauperien Action Revisited" 1994 *SALJ* 47.

156 *Kruger v Coetzee* 1966 2 SA 428 (A).

157 Scott "Harm by Animals: the South African Law through the Cases, JF Uys" 2017 *SALJ* 712–714.

158 *Van Meyeren v Cloete* [2020] ZASCA 100 (11 September 2020).

159 The approach to liability for animals is linked to the concept of lack of predictability and, therefore, interesting to that extent in the context of autonomous behaviour. Safety legislation will play an important role in reducing this unpredictability to a socially accepted minimum.

160 The number of stakeholders involved in the creation and operation of AI systems may include hardware manufacturers, software designers, sellers, equipment and software installers, facility owners, AI owners, AI users and trusted third parties, amongst others — allocating liability in this context is not an easy feat.

causal link in delictual claims or a link between defect and damage in product liability claims.[161] However, given that each EDT's thought processes are unique and will mostly be unsupervised, the respondent may escape delictual liability if they can demonstrate that the EDT was developed correctly and tested before release, that their employees and auxiliaries were well trained and supervised, and that they implemented proper quality control mechanisms before release in the supply and value chain.

Even if one can identify a fault from a human stakeholder interacting with EDT, the lack of predictability may intercept the causation link between this human's fault and the injured victim. Emerging technologies' lack of predictability poses similar problems under product liability principles, as manufacturers are only liable for defects or inadequate instructions when the product poses a predictable risk of harm. As such, one will be hard-pressed to find a producer liable under the South African product liability doctrine.

Product liability may facilitate the allocation of liability by prescribing joint liability to the stakeholders; however, the current provisions on joint liability may not adequately protect all relevant stakeholders in an EDT assembly, supply, and value chain. Moreover, even in strict liability cases, it is necessary to determine which of the stakeholders along these EDT chains can be held liable, which may prove impossible when EDT autonomously acts due to its external stimuli.

In addition, EDT is continuously altered after its launch into the consumer market as new data is uploaded, open-source software is updated, or patches are applied by the manufacturer, the consumer, the EDT itself, manufacturers of individual system components, or third parties.[162] These new updates add or remove features that change the risk profile of the EDT initially released by the manufacturers and affect the behaviour of the entire EDT system.

Autonomy of EDT means that humans have less control, rendering the general liability principles of agency, control, and foreseeability moot. Even more so under the common law of delict, determining how and when manufacturers, operators, and/or users of EDT may commit a breach of duty or a fault and establishing causation is not simple. It needs to be determined who may be held liable in cases where EDT decisions are not directly related to human inputs but rather a result of EDT's interpretation of reality or, even if a human had played a role in causing damage (the programmer instructed EDT to take a specific type of data into account) . If EDT learned from its surrounding external inputs, adjusted to improve its efficiency, and then committed a delict, it is questionable if "fault" or "breach of duty" should remain elements to prove or disprove under delictual claims.

Presiding officers will be confronted with liability claims arising from EDT's actions, during which they must attempt to determine which legal entity may be responsible for the damage caused by these actions.

Even if the plaintiff, burdened to prove causation, may ultimately recover the expenses of employing an expert witness, it may be a bar to pursuing the claim. Also, more than one stakeholder may be liable for EDT delicts, which must be premised on a balance of probabilities.

161 In the context of judicial proceedings, if a plaintiff cannot go back to the chain of data processing and recreate the circumstances of AI's reasoning process to understand what led to a specific (faulty) output, its action may very well be doomed as he/she will not be able to fulfil the basic evidentiary requirements regarding fault and causation.

162 There is an implied provision that the producer or importer, the distributor and the retailer each warrant that the goods comply with the relevant requirements and standards. There is an implied warranty of quality in any transaction or agreement about the supply of goods to a consumer (s 56, CPA). Under this section, the producer, importer, distributor and retailer each warrant that the goods comply with the requirements and standards contemplated in s 55 of the CPA, except to the extent that those goods have been altered contrary to instructions or after leaving the control of the producer, importer, distributor or retailer.

Proportionality of the claim may then also, in matters concerning multiple stakeholders, vary in cases where joint and several liability of all those to whom are liable for EDT caused harm.

Suppose the technology whose implementation led to harm falls under a strict liability doctrine, such as product or vicarious liability. In that case, the plaintiff only needs to prove that the patrimonial damage resulted from the operation of the EDT and not the exact processes within it that caused harm. If the claim is based on fault liability instead, the chain of causation must be drawn back beyond the operation of the EDT to a person controlling it or even further back.[163] It does not suffice to point to any conduct of that person merely, but it must be faulty, so the events leading to the damage at stake must be researched much more thoroughly.

Applying product liability principles to stakeholders of autonomous EDT could stifle innovation if delictual principles hold them liable for actions over which they have no control. Humans causing delicts in similar cases could rebut liability claims without fault or negligence.

For product liability to find any consideration, one should determine if EDT is indeed a "product". It was stated that the word "goods" is used under the CPA. Although "goods" may be defined broadly, this only concerns tangible movables, which means hardware, thus excluding EDT as software and algorithms, which are most often considered services, not goods.[164] With computer software, a service is software that performs automated tasks, responds to hardware instructions, or responds to data requests from other software. In a user's operating system, these services are often loaded automatically at start-up and run in the background without user interaction. Software responds to the user's keyboard inputs, indexes and optimises the file system, and communicates with other devices on the network. A computer program is defined in the Copyright Amendment Act as "a set of instructions that is fixed or stored in any manner and which, when used directly or indirectly in a computer, directs its operation to bring about a result".[165] Thus, algorithms are excluded from product liability.

Lastly, as for vicarious liability, it is evident that the past and current definitions of an "employee" refer to a "person", a legal entity that could serve as per agreement and earn money or in kind. This excludes EDT. Thus, our legislation and common law doctrine of vicarious liability regarding EDT return to the position prevalent before the LRA of 1956.

The *actio de pauperie* does seem to provide guidelines. This common law doctrine applies where harm is caused by no fault of the animal's owner. Strict liability is thus imposed on the owner of the domestic animal.[166] However, it will be an unreasonable rebuttal for the owner to prove that the animal (or in the case of this topic, EDT) acted outside of its normal expected behaviour.

Against this backdrop, it will be increasingly difficult to pinpoint who may be held responsible when EDT causes civil delictual damage. It will be a far cry from causality under strict liability principles to assign liability to a manufacturer or supplier whose EDT was detached in both time and geographic location from the completion and operation of the original EDT. This is the current position in South Africa.

Fortunately, the EU has set the benchmark for these cases.

163 Koch *Journal of European Tort Law* 124.

164 See s 1 of CPA for the definition of "goods".

165 Copyright Amendment Act 125 of 1992, s 1.

166 The approach to animal liability is linked to the lack of predictability and is interesting in the context of autonomous behaviour. Safety legislation will be important in reducing this unpredictability to a socially accepted minimum.

6 INTERNATIONAL DEVELOPMENTS: EUROPEAN UNION

6 1 Background

The EU took the initiative to consider applying member states' existing regulations to EDT and formulate conclusions regarding the need for legislative changes.[167] Herewith is a short summary of the EU initiatives in chronological order relating to the intended regulation of AI. This summary will also include identifying the key factors considered.

As recently as 2017, the European Parliament found it "appropriate, given the stage reached in the development of robotics and AI, to start with civil liability issues" and passed the Resolution on Civil Law Rules on Robotics (the EU AI Resolution).[168] This called for a legislative policy on the liability of *inter alia* AI.[169] The European Parliamentary Research Service (EPRS) then produced a study on "[a] common EU approach to liability rules and insurance for connected and autonomous vehicles," which was published one year after the EU AI Resolution.[170] By then, the EU had already announced that it would focus on EDT due to its increasing role in the economy and society.[171] A Joint Declaration of the Presidents of the Commission, Parliament, and Council had pledged to ensure high data protection, digital rights, and ethical standards while capturing the benefits and avoiding risks.[172] The EU published its Communication on Artificial Intelligence for Europe,[173] accompanied by a Staff Working Document on Liability for emerging digital technologies (the EU Liability Document 2019) in the first quarter of 2018.[174] In this Communication, the EU *inter alia* announced that it would assess "whether the safety on national and EU liability frameworks are fit for purpose in light of the challenges of AI, as spearheaded by the Expert Group on Liability and New Technologies — New Technologies Formation."[175] Furthermore, "[f]or the purposes of liability, it is not necessary to give autonomous systems a legal personality".[176]

Since then, the EU has repeatedly confirmed that it will pursue its plan and "continue work on the emerging challenge of EDT by enabling coordinated action across the European Union".[177] Its most recent work program for 2020 emphasised the "need to establish an ecosystem of trust

167 Ziemianin *Internet Policy Review*. See also Reimann "Product Liability in a Global Context: The Hollow Victory of the European Model" 2003 *European Review of Private Law*.

168 This was published on 16 February 2017.

169 Civil Law Rules on Robotics TA (europa.eu) (accessed 04-06-2024).

170 Press-room "MEPs Call for Safety and Liability Rules for Driverless Cars" https://www.europarl.europa.eu/ news/en/press-room/20190109IPR23013/meps-call-for-safety-and-liability-rules-for-driverless-cars (accessed 04-05-2022); Koch *Journal of European Tort Law*.

171 European Commission "Commission Work Programme 2018 – COM (2017) 650 final, 3f" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A650%3AFIN (accessed 04-05-2022).

172 *Ibid*.

173 European Commission "European Approach to Artificial Intelligence" https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence#:~:text=The%20AI %20strategy%20proposed%20measures,global%20hub%20for%20trustworthy%20AI (accessed 04-06-2024).

174 EU Staff Working Document: Liability for Emerging Digital Technologies.

175 EUR-Lex "Communication from the Commission Artificial Intelligence for Europe" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018 %3A237%3AFIN 16 (accessed 04-05-2024).

176 Expert Group on Liability and New Technologies – New Technologies Formation "Liability for Artificial Intelligence and other Emerging Digital Technologies" para 8 https://data.europa.eu/doi/10.2838/573689 (accessed 07-06-2022).

177 European Commission "Commission Work Programme 2019, COM (2018) 800 final" cwp_2019_publication_en.pdf (europa.eu) (accessed 07-06-2022).

to ensure it develops within clearly defined ethical boundaries".[178] In 2020, the EU published a bundle of documents, particularly the White Paper: Artificial Intelligence — A European Approach to Excellence and Trust[179] and The Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics (the Report on AI liability).[180]

6 1 1 Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics

The report on AI liability identified the possible challenges AI poses to existing EU liability rules. At the EU level, product safety and product liability provisions[181] are two mechanisms to pursue the same policy goal of high levels of safety: minimising the risk of harm to users and providing compensation for damages resulting from defective goods.[182] At the national level, non-harmonised civil liability frameworks complement these rules by ensuring compensation for damages from various causes and addressing different liable persons, including owners, operators, or service providers.[183] The safety section builds on the Machinery Directive and the work with the relevant expert groups.[184] The liability section builds on evaluating the Product Liability Directive and the input of the appropriate expert groups[185] and stakeholders.[186] Although improving EU safety rules for EDT could facilitate avoiding accidents, they may happen. This is when civil liability intervenes.[187]

Liability frameworks in the EU rely on the parallel application of the Product Liability Directive and other non-harmonised national liability regimes. The Product Liability Directive provides protection that national fault-based liability alone does not provide. It imparts strict liability to the producer for damage caused by a defect in their products.[188] In case of physical or material damage, the injured party is entitled to compensation if they prove the damage, the defect in the product (i.e., that it did not provide the safety that the public is entitled to expect), and the causal

178 European Commission "Commission Work Programme 2020, COM (2020) 37 final" https://eur-lex.europa.eu/resource.html?uri=cellar:7ae642ea-4340-11ea-b81b-01aa75ed71a1.0002.02/DOC_1&format=PDF (accessed 04-05-2022).

179 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0065&WT_mc_id=Twitter; resource.html (europa.eu) (accessed 04-05-2022).

180 https://ec.europa.eu/info/publications/commission-report-safety-and-liability-implications-ai-internet-things-and-robotics-0_en (accessed 04-05-2022).

181 Although the Product Liability Directive's definition of product is broad, its scope could be further clarified to better reflect the complexity of emerging technologies and ensure that compensation is always available for damage caused by defective products due to software or other digital features. This would better enable economic actors, such as software developers, to assess whether they could be considered producers according to the Product Liability Directive.

182 The EU AI report.

183 *Ibid*.

184 Consumer Safety Network established in Directive 2001/95/EC on General Product Safety (GPSD), Machinery Directive 2006/42/EC and Radio Equipment 2014/53/EU Directive expert groups composed of member states, industry and other stakeholders such as consumer associations.

185 The Expert Group on Liability and New Technologies was created to provide the Commission with expertise on the applicability of the Product Liability Directive and national civil liability rules and with assistance in developing guiding principles for possible adaptations of applicable laws related to new technologies. It consists of two formations, the "Product Liability Formation" and the "New Technologies Formation", see http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3592&NewSearch=1&NewSearch=1 (accessed 04-05-2024). For the "'New Technologies Formation' Report on Liability for Artificial Intelligence and Other Emerging Technologies" see https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199 (accessed 04-05-2024).

186 The EU AI report.

187 *Ibid*.

188 *Ibid*.

link between the defective product and the damage. Thus, strict liability.

National non-harmonised regimes provide fault-based liability rules. In these cases, the damage victims must prove the fault of the liable person, the damage, and the causality between the fault and the damage to establish a successful liability claim.[189] They also provide strict liability regimes where the national legislator has attributed liability for a risk to a specific person without needing a victim to prove fault/defect or causality between fault/defect and the damage. This is thus a more strenuous and costly evidentiary burden than that of strict liability.[190]

National liability regimes provide victims of damage caused by products and services with several parallel compensation claims premised on fault or strict liability. These claims are directed against different liable persons and have different requirements.[191]

However, the characteristics of EDT challenge aspects of EU and national liability frameworks and could impede their effectiveness. It would be difficult to follow the nexus of the damage back to human behaviour, which could give grounds for a fault-based claim in national rules.[192] This means that liability claims based on national tort laws may be difficult or costly to prove. Victims of EDT products and services accidents must not enjoy a lower level of protection than similar products and services for which they would get compensation under national tort law.

A short explanation follows of how EDT challenges the EU frameworks and what the Expert Groups suggested as solutions.

6 1 1 1 Complexity of Products, Services and the Value-chain

The EU acknowledged that the dividing line between products and services may no longer be as clear-cut as it was. Software and EDT merit specific attention in respect of product liability. Software is essential to the functioning of many EDT products and may affect their safety. It is integrated into products, but it may also be supplied separately to enable the use of the product as intended.[193] This means that software can make a tangible product defective and cause damage. This could result in the product producer being liable under the Product Liability

189 The EU AI report.

190 *Ibid*.

191 For instance, a victim involved in a car accident typically has a strict liability claim against the owner of the car (i.e., the person who takes out motor vehicle liability insurance) and a fault-based liability claim against the driver, both under national civil law, as well as a claim under the PDL against the producer if the car had a defect. Following the harmonised rules on motor vehicle insurance, the use of the vehicle must be insured (Harmonised for motor vehicles by Directive 2009/103/EC relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability) and the insurer is always the first point of the claim for compensation for personal injury or material damage. According to these rules, the obligatory insurance compensates the victim and protects the insured person who is liable under national civil law rules (in most member states strict liability is applied for the person in whose name the motor vehicle is registered) to pay financial damages for the accident involving the motor vehicle. Producers are not subject to mandatory insurance under the Product Liability Directive. In EU legislation, autonomous vehicles are not treated any differently from non-autonomous vehicles regarding motor insurance. Like all vehicles, such vehicles must be covered by third-party motor liability insurance, which is the easiest way for the injured party to get compensation. Proper insurance can mitigate the negative consequences of accidents by providing smooth compensation for the victim. Clear liability rules help insurance companies calculate risks and claim reimbursement from the party ultimately liable for the damage. For example, if a defect causes an accident, the motor insurer can claim reimbursement from the manufacturer after compensating the victim.

192 The EU AI report.

193 *Ibid*.

Directive.[194]

However, as software comes in many forms, answers related to software classification as a service or product may sometimes take more work. Thus, while software steering the operations of a tangible product could be considered part or component of that product, some forms of stand-alone software could be more challenging to classify.[195] Emerging digital technology applications are often integrated into complex environments where many connected devices and services network. The combination of different digital components in a complex ecosystem and the variety of actors involved can make it difficult to assess where potential damage originates and which person is liable for it.[196] Due to the complexity of these technologies, it can be complicated for victims to identify the liable person and prove all necessary conditions for a successful claim, as required under national law. The costs for this expertise may be monetarily prohibitive and discourage victims from claiming compensation.

In addition, products and services relying on EDT will interact with traditional technologies, leading to added complexity in liability.[197] For example, autonomous cars will share the road with traditional ones for a specific time. Similar complexity of interacting actors will arise in some service sectors where partially automated EDT systems will support human decision-making.[198]

According to the Report[199] from the New Technologies formation of the Expert Group, adaptations of national laws to facilitate the burden of proof for the victims of EDT-related damage should be considered. For example, the burden of proof could be linked to compliance by a relevant operator with specific cybersecurity or other safety obligations set by law. If a user of EDT does not comply with these rules, a change to the burden of proof regarding fault and causation could apply.[200]

6 1 1 2 Connectivity and Openness

According to the Expert Group, it needed to be clarified what safety expectations may be regarding the damage that results from cybersecurity breaches in the product and whether such damage would be adequately compensated under the Product Liability Directive. Cybersecurity weaknesses may exist from the outset when an EDT product is put into circulation. They may also appear later after the product is put into circulation. In fault-based liability frameworks, establishing clear cybersecurity obligations allows the operators to determine what they must do to avoid the consequences of liability.[201]

Under the Product Liability Directive, the question of whether a producer could have foreseen specific changes taking account of the product's reasonably foreseeable use may become more critical, as was suggested by the Expert Group. Here, three suggestions were tabled: first, one might apply the "later defect defence".[202] Here, producers may not be held liable if the defect did not exist when the product was put into circulation. Second, the "development risk defence"

194 *Ibid*.

195 The EU AI report.

196 *Ibid*.

197 *Ibid*.

198 *Ibid*.

199 Liability for Artificial Intelligence and Other Emerging Technologies' Report https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199 (Expert Group Report) (accessed 04-05-2024).

200 The EU AI report.

201 *Ibid*.

202 *Ibid*.

where the state-of-the-art knowledge at the time could not have foreseen the defect.[203] And third, liability could be reduced if the injured party did not perform safety-relevant updates. This could be regarded as contributory negligence by the injured person, reducing a producer's liability.[204] As the notion of foreseeable reasonable use and questions of contributory negligence may become more prevalent, injured persons might find it more challenging to obtain compensation for damage caused by a defect in a product.[205]

6 1 1 3 Autonomy and Opacity

Where EDT applications can act autonomously, they eventually perform tasks without being pre-defined by humans and algorithms.[206] Algorithms based on machine learning can be complex to understand. This is known in the tech field as the so-called "black-box-effect".[207]

In addition to the complexity discussed above, due to the black-box-effect in some EDTs, obtaining compensation for damage caused by autonomous EDT applications could become problematic. Understanding the algorithm and the data used by the EDT requires analytical capacity and technical expertise, which victims could find costly.[208] In addition, access to the algorithm and the data could only be possible with the cooperation of the potentially liable party.[209] In practice, victims may thus not be able to make a liability claim easily. Also, it would be unclear how to demonstrate the fault of an EDT acting autonomously or what would be considered the fault of a person relying on EDT.[210]

The EU's national laws have already developed several solutions to reduce the burden of proof for victims in similar situations. A guiding principle for EU product safety and liability remains that producers must ensure that all products put on the market are safe throughout their life-cycle and for the product that can reasonably be expected.[211] A manufacturer must ensure that a product using EDT respects specific safety parameters. The features of EDT do not prevent an entitlement to safety expectations for products, whether they are automatic cars or surgery robots.[212]

Autonomy can affect a product's safety as it may substantially alter its characteristics and safety features. Under what conditions do self-learning features prolong the producer's liability, and to what extent should the producer have foreseen specific changes?[213]

In close coordination with corresponding changes in the EU safety framework, The Expert Group suggested revisiting the notion of "putting into circulation" applied in the Product Liability Directive to account for the possibility of products changing and altering.[214] This could

203 *Ibid*.

204 The EU AI report.

205 *Ibid*.

206 *Ibid*.

207 https://www.techopedia.com/definition/34940/black-box-ai (accessed 04-05-2024). Black box AI is any AI so complex that its decision-making process cannot be explained in a way humans can easily understand. Black box AI is the opposite of explainable AI. Black box AI is undesirable for several reasons. When the internal workings of an AI system are not understood, it becomes increasingly challenging to identify why an AI model is producing biased outputs and where errors in logic are occurring. It also makes it difficult to determine who should be held accountable when outputs are flawed or outright dangerous.

208 The EU AI report.

209 *Ibid*.

210 *Ibid*.

211 *Ibid*.

212 *Ibid*.

213 *Ibid*.

214 The EU AI report.

clarify who may be liable for any changes made to the product.

6 1 1 4 Risk Profile

The Expert Group Report also provided that the operation of some EDT could have a specific risk profile in terms of liability as they may cause significant harm to vital human interests such as life, health, and property and expose the public to risks.[215] This could mainly concern EDT that move in public spaces, for example, fully autonomous vehicles, drones[216] and package delivery robots or EDT-based services with similar risks.[217] The challenges of autonomy and opacity to national tort laws could be addressed following a risk-based approach. Strict liability regulations could guarantee that the victim is compensated whenever the risk occurs, regardless of fault. The impact of choosing who should be strictly liable for such operations on the development and uptake of EDT needed to be evaluated, and a risk-based approach should be considered.[218]

While the existing EU and national liability laws could, in principle, cope with EDT, the dimension and combined effect of the challenges of EDT could make it more difficult to offer victims compensation in all cases where this would be justified.[219] Thus, allocating the cost when damage occurs may be unfair or inefficient under the then-current rules. To rectify this and address potential uncertainties in the existing framework, specific adjustments to the Product Liability Directive and national liability regimes through appropriate EU initiatives were to be considered using a targeted, risk-based approach, i.e., considering that different EDT applications pose different risks.[220]

6 2 Enactment of the Regulatory Framework for EDT: the AI Act and Directives

Considering the above comments and suggestions of the Expert Group, in early May 2024, the EU gave final agreement to the world's first significant law regulating EDT: the Artificial Intelligence Act 2024 (the AI Act). The AI Act is not a standalone piece of legislation but should be seen in the broader context of the EU's approach to ensure effective regulation of EDT. In addition, in September 2022, the EU Commission published a proposed package of additional regulatory measures to support the rollout of EDT within Europe.[221] This package comprised the proposed AI Liability Directive (AILD)[222] and the proposed Product Liability Directive (PLD) revisions.[223] These twin directives form part of the EU's regulatory framework on EDT,

215 *Ibid*.

216 Expert Group Report.

217 The EU AI report.

218 *Ibid*.

219 See the New Technologies Formation Report, 3, and the policy recommendation 27.2. of the High-Level Expert Group on Artificial Intelligence, which is crucial for addressing the challenges of AI liability.

220 The EU AI report.

221 Launders "Beyond the AI Act: The AI Liability Directive & the Product Liability Directive"https://www.techlaw.ie/2024/03/articles/artificial-intelligence/beyond-the-ai-act-how-the-ai-liability-directive-and-the-product-liability-directive-will-also-shape-the-regulation-of-ai-in-the-eu/ (accessed 04-05-2024).

222 EUR-Lex "Proposal for a Directive of the European Parliament and of the Council on Adapting Non-contractual Civil Liability Rules to Artificial Intelligence (AI Liability Directive)" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0496 (accessed 04-05-2024).

223 https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.pdf (accessed 04-05-2024).

in conjunction with the AI Act.

The AI Act is, in part, product safety legislation. One of its primary purposes is to minimise risks associated with EDT systems before they are placed on the market or deployed.[224]

The cumulative effect of the AI Act, AILD, and PLD is that where a product causes a person's injury, different legal avenues for claiming compensation will be available to them.[225] These claims may be contractual claims or claims for non-contractual civil liability. Alternatively, the injured party may have recourse under strict liability regimes, such as the defective product liability regime. In developing the AILD and the PLD, the Commission has focused on (i) strict liability for defective products, and (ii) non-contractual civil liability claims.[226]

6 2 1 The AI Act

The AI Act establishes obligations for providers and users depending on the level of risk from EDT, specifically AI. This Act classifies AI according to its risk:

i. Prohibited risk AI systems are considered a threat to people and are prohibited. This is regulated in Chapter II, Article 5. They include:

- deploying subliminal, manipulative, or deceptive techniques to distort behaviour and impair informed decision-making, causing significant harm;
- exploiting vulnerabilities related to age, disability, or socio-economic circumstances to distort behaviour, causing significant harm;
- biometric categorisation systems inferring sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation), except labelling or filtering of lawfully acquired biometric datasets or when law enforcement categorises biometric data;
- social scoring, that is, evaluating or classifying individuals or groups based on social behaviour or personal traits, causing detrimental or unfavourable treatment of those people;
- assessing the risk of an individual committing criminal offences solely based on profiling or personality traits, except when used to augment human assessments based on objective, verifiable facts directly linked to criminal activity;
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage;
- inferring emotions in workplaces or educational institutions, except for medical or safety reasons;
- "real-time" remote biometric identification in publicly accessible spaces for law enforcement, except when:
    - ○ searching for missing persons, abduction victims, and people who have been human

224 Launders "Beyond the AI Act".

225 PLD note 9: "Under the legal systems of the Member States, an injured person could have a claim for damages based on contractual liability or on the grounds of non-contractual liability that do not concern the manufacturer's liability for the defectiveness of a product as established in this Directive. This concerns, for example, liability based on a warranty or fault or strict liability of operators for damage caused by the properties of an organism resulting from genetic engineering. Such provisions, which serve to attain, inter alia, the objective of effective protection of consumers and other natural persons, should remain unaffected by this Directive."

226 Launders "Beyond the AI Act".

trafficked or sexually exploited;

○ preventing substantial and imminent threat to life or foreseeable terrorist attack; or

○ identifying suspects in serious crimes.

ii. High-risk AI systems that negatively affect safety or fundamental rights are divided into two categories. High-risk AI systems are those articulated in Chapter III, Article 6:

- used as a safety component or a product covered by EU laws in Annex I[227] and required to undergo a third-party conformity assessment under those Annex I laws or
- those under Annex III[228] use cases (below), except if:

  ○ the AI system performs a narrow procedural task;

  ○ improves the result of a previously completed human activity;

  ○ detects decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment without proper human review; or

  ○ performs a preparatory task to an assessment relevant to the purpose of the use cases listed in Annex III.

AI systems that profile individuals are considered high-risk. This entails automated processing of personal data to assess various aspects of a person's life, such as work performance, economic situation, health, preferences, interests, reliability, behaviour, location, or movement.[229]

Articles 8–17 provide the compulsory requirements for providers of high-risk AI systems. High-risk AI providers must:

- establish a risk management system throughout the high-risk AI system's life cycle;
- conduct data governance, ensuring that training, validation, and testing datasets are relevant, sufficiently representative, and, to the best extent possible, free of errors and complete according to the intended purpose;
- draw up technical documentation to evidence compliance and provide authorities with the information to assess that compliance;
- design their high-risk AI system to automatically record events relevant to identifying national-level risks and substantial modifications throughout its lifecycle;
- provide instructions for future deployers to enable the latter's compliance;
- design their high-risk AI system to allow deployers to implement human oversight;
- design their high-risk AI system to achieve appropriate accuracy, robustness, and cybersecurity levels;
- establish a quality management system to ensure compliance.

Most obligations fall on developers of high-risk AI systems. This pertains to those that intend to

227 EU Artificial Intelligence Act Annex I: List of Union Harmonisation Legislation | EU Artificial Intelligence Act.

228 EU Artificial Intelligence Act Annex III: High-Risk AI Systems | EU Artificial Intelligence Act.

229 AI Act Overview artificialintelligenceact.eu https://artificialintelligenceact.eu/wp-content/uploads/2024/05/AI-Act-overview-30.05.2024.docx (accessed 04-05-2024).

place on the market or put into service high-risk AI systems in the EU, regardless of whether they are based in the EU or a third country.[230] This also includes third-country providers where the high-risk AI system's output is used in the EU. All high-risk AI systems will be assessed before being put on the market and throughout their lifecycle. Generative AI will not be classified as high-risk but must comply with transparency requirements and EU copyright law.[231] This entails disclosing that the content was generated by AI, designing the model to prevent generating illegal content, and publishing summaries of copyrighted data applied for training. High-impact general-purpose AI models that might pose systemic risk, such as the more advanced AI model GPT-4, would have to undergo thorough evaluations, and any severe incidents would have to be reported to the European Commission. Content generated or modified with the help of AI — images, audio, or video files (for example, deepfakes) — need to be clearly labelled as AI-generated so that users are aware.

iii. Minimal-risk systems, such as AI-enabled video games and spam filters, are unregulated; however, this is changing with generative AI, and developers must be classified as high-risk should they wish to release their product to the public.

6 2 2 Revised Products Liability Directive

The EU initially adopted the PLD in 1985.[232] This directive was premised on a strict liability regime for material damage suffered due to the use of defective products. Following an evaluation of the PLD in 2018, the EU Commission found that while it was an effective instrument, it required an update suitable for the digital age. Following informal negotiations in December 2023, the EU institutions reached a political agreement on a compromise text. The compromise text was recently approved by Parliament committees and is put before the Parliament for a vote. It will then pass to the Council for approval and adoption if approved.[233]

The proposed reform of this directive is extended beyond a mere update to account for EDT. These changes include a general widening in scope of application, including a more

230 "AI Act Consolidated Text" https://artificialintelligenceact.eu/wp-content/uploads/2024/01/AI-Act-Overview_24-01-2024.pdf. (accessed 04-05-2024).

231 European Parliament "EU AI Act: First Regulation on Artificial Intelligence" https://www.europarl.europa.eu/pdfs/news/expert/2023/6/story/20230601STO93804/20230601STO93804_en.pdf. (accessed 04-05-2024).

232 EUR-Lex "Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations, and administrative provisions of the Member States concerning liability for defective products" https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31985L0374 (accessed 04-05-2024).

233 The compromise text sets out a lead time of 24 months for member states to implement the directive in national law, which means businesses and individuals should expect to have local laws implemented in 2026 (if the PLD enters into force this year). This lead time would align with the AI Act, which is also set at 24 months following its entry into force. The alignment means that those preparing for compliance with the AI Act should also consider how the PLD will interact alongside it, bearing in mind that the PLD will need to be transposed into the local laws of each member state. In contrast, the AI Act will apply directly as an EU Regulation.

comprehensive definition of "product"[234] and "liable parties."[235]

The first is an explicit acknowledgment that AI systems fall within the scope of the PLD, under the inclusion of "*software*"[236] within the definition of "*product*"; however, it excludes "information":

> In the interest of legal certainty, it should be clarified in this Directive that software is a product to apply no-fault liability, irrespective of the mode of its supply or usage, … Information is not, however, to be considered a product, and product liability rules should therefore not apply to the content of digital files, such as media files or e-books or the source code of software.[237]

Under this extended scope, AI system providers might be liable for any defective AI systems placed on the market. It also covers any AI systems integrated into products, clouding the traditional distinction between tangible and intangible products. While the PLD will not

234 PLD art 1: "(1) 'product' means all movables, even if integrated into, or inter-connected with, another movable or an immovable; it includes electricity, digital manufacturing files, raw materials and software."

235 PLD note 33: "The protection of natural persons requires that any manufacturer involved in the production process can be held liable, in so far as a product or a component supplied by that manufacturer is defective. This includes any person who presents themselves as the manufacturer by putting, or authorizing a third party to put, their name, trademark, or other distinguishing feature on a product, since by doing so, that person gives the impression of being involved in the production process or of assuming responsibility for it. Where a manufacturer integrates a defective component from another manufacturer into a product, an injured person should be able to seek compensation for the same damage from the manufacturer of the product, the manufacturer of the component, or both. Where a component is integrated into a product outside the control of the manufacturer of that product, an injured person should be able to seek compensation from the component manufacturer where the component itself is a product under this Directive." PLD Art 38: "Online selling has grown consistently and steadily, creating new business models and new actors in the market such as online platforms. Regulation (EU) 2022/2065 of the European Parliament and of the Council 14 and Regulation (EU) 2023/988 regulate, *inter alia*, the responsibility and accountability of online platforms concerning illegal content, including to the sale of products. When online platforms perform the role of manufacturer, importer, authorized representative, fulfillment service provider, or distributor regarding a defective product, they should be subject to the same liability as such economic operators. Where online platforms play a mere intermediary role in selling products between traders and consumers, they are covered by a conditional liability exemption under Regulation (EU) 2022/2065. However, Regulation (EU) 2022/2065 establishes that online platforms that allow consumers to conclude distance contracts with traders are not exempt from liability under consumer protection law where they present the product or otherwise enable the specific transaction in question in a way that would lead an average consumer to believe that the product is provided either by the online platform itself or by a trader acting under its authority or control. In keeping with that principle, when online platforms so present the product or otherwise enable a specific transaction, it should be possible to hold them liable in the same way as distributors under this Directive. Therefore, provisions of this Directive relating to distributors should apply mutatis mutandis to such online platforms. That means that such online platforms should be liable only when they present the product or otherwise enable the specific transaction in a way that would lead an average consumer to believe that the product is provided either by the online platform itself or by a trader acting under its authority or control, and only where the online platform fails to identify a relevant economic operator established in the Union promptly."

236 PLD note 6: "To ensure that the Union's product liability regime is comprehensive, no-fault liability for defective products should apply to all movables, including software, including when they are integrated into other movables or installed in immovables."

237 PLD notes 13 and 16: "Whereas digital files as such are not products within the scope of this Directive, digital manufacturing files, which contain the functional information necessary to produce a tangible item by enabling the automated control of machinery or tools, such as drills, lathes, mills, and 3D printers, should be considered to be products, to ensure the protection of natural persons in cases where such files are defective. For example, a defective computer-assisted design file used to create a 3D-printed good that causes harm should give rise to liability under this Directive, where such a file is developed or supplied in the course of a commercial activity. For the avoidance of doubt, it should be clarified that raw materials, such as gas and water, and electricity are products."

apply to free and open-source software supplied outside the course of commercial activity,[238] manufacturers that integrate free and open-source software into their products are potentially liable for any defects that may result.[239]

Articles 17 and 18 of the PLD provide that, although it does not apply to services, digital services are frequently integrated into, or inter-connected with, a product so that the absence of the service would prevent the product from performing one of its functions. Thus, it is necessary to extend no-fault liability to integrated or inter-connected digital services ("related services")[240] as they determine the product's safety just as much as physical or digital components. Those related services should be considered components of the product into which they are integrated or inter-connected.[241]

The PLD provides for the recovery of any material losses resulting from a product defect, while the laws of each member state determine compensation for non-material losses.[242] The concept of "*damage*" in the PLD has also been broadened in several ways.[243] For example, Article 6(1)(b)(iii) provides that loss or corruption of data is now recoverable, except if the data is used for professional purposes. The compromise text clarifies that destruction or corruption of data does not automatically result in material loss if an injured party can still retrieve the data at no cost. Damage to any property that is not used for professional purposes remains non-recoverable.[244]

This widened scope of damage will increase the potential liability of AI system providers in the context of AI systems. It also clarifies that certain types of damage, such as privacy infringements, will not trigger liability under the PLD.[245] Notably, the compromise text widens the availability of compensation rights to indirect victims who suffer damage because of direct victims' damage.[246]

The concept of defectiveness under the PLD has also been updated to account for AI systems.[247] In addition, one can see the self-learning nature of the product as a factor for courts to consider when assessing defectiveness, which should be determined "by reference not to its fitness for

238 PLD note 14: "Free and open-source software, whereby the source code is openly shared, and users can freely access, use, modify and redistribute the software or modified versions thereof, can contribute to research and innovation on the market. Such software is subject to licences that allow anyone to run, copy, distribute, study, change, and improve the software. To not hamper innovation or research, this Directive should not apply to free and open-source software developed or supplied outside the course of commercial activity, since products so developed or supplied are by definition not placed on the market."

239 PLD note 15: "Where free and open-source software supplied outside the course of a commercial activity is subsequently integrated by a manufacturer as a component into a product in the course of a commercial activity and is thereby placed on the market, it should be possible to hold that manufacturer liable for damage caused by the defectiveness of such software but not the manufacturer of the software because they would not have fulfilled the conditions of placing a product or component on the market."

240 PLD art 1(3): "'related service' means a digital service that is integrated into, or inter-connected with, a product in such a way that its absence would prevent the product from performing one or more of its functions."

241 European Parliament "Texts Adopted – Liability for Defective Products, Tuesday, 12 March 2024" https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.html (accessed 04-07-2024).

242 PLD note 23.

243 PLD note 20.

244 PLD note 22: "In order to address a potential risk of litigation in an excessive number of cases, the destruction or corruption of data that are used for professional purposes, even if not exclusively so, should not be compensated under this Directive."

245 PLD notes 24 and 25.

246 PLD note 27: "In so far as national law provides, the right to compensation for injured persons should apply both to direct victims, who suffer damage directly caused by a defective product, and to indirect victims, who suffer damage as a result of the direct victim's damage." https://www.europarl.europa.eu/doceo/document/TA-9-2024-0132_EN.pdf (accessed 04-03-2024).

247 Launders "Beyond the AI Act".

use but to the lack of the safety that a person is entitled to expect or that is required under EU or national law".[248] This requires an objective analysis of the safety that the public at large is entitled to expect and not that which an individual might expect. This expectation should be assessed by considering, *inter alia*, "the intended purpose, reasonably foreseeable use,[249] presentation, objective characteristics and properties of the product in question, including its expected lifespan, and the specific requirements of the group of users for whom the product is intended"[250] … and "its failure to fulfil [its] purpose".[251]

In addition, the court should consider the product's presentation. Warnings or other information provided with a product cannot be deemed adequate to make an otherwise defective product safe.[252] Liability under the PLD cannot be circumvented simply by listing all possible product side effects. When determining a product's defectiveness, reasonably foreseeable use also encompasses misuse that is not unreasonable under the circumstances, such as the foreseeable behaviour of an EDT user resulting from a lack of concentration or the foreseeable behaviour of particular user groups, such as children.[253] It should be possible for a court to find that a product is defective without establishing its actual defectiveness, where it belongs to the same production series as a product already proven to be faulty.[254]

Products can also be considered "*defective*" because of cybersecurity vulnerabilities, which will be particularly relevant in using and deploying AI systems.[255] An updated recital in the compromise text outlines that manufacturers who design products that can develop unexpected behaviour remain responsible for behaviour that causes damage. In the context of AI systems, this would indicate that the ability of a system to act unexpectedly will not be enough for a developer to excuse itself from liability. The actions or omissions of third parties will also not excuse AI system providers from liability where a defect exists in the product. This could be where a third party exploits a cybersecurity vulnerability in an AI system that results in damage suffered. Conversely, the liability of AI providers can be reduced or disallowed where the injured party themselves contributed to the damage, such as failing to install updates or upgrades to the AI system.

The traditional defense under the PLD that the defect in the product arose after being placed on the market (the so-called "development risk defense") has a new addition to account for the fact

248 PLD note 28.

249 PLD note 46: "Reasonably foreseeable use covers the use for which a product is intended under the information provided by the manufacturer or economic operator placing it on the market, the ordinary use as determined by the design and construction of the product, and use which can be reasonably foreseen where such use could result from lawful and readily predictable human behaviour."

250 PLD note 28.

251 PLD note 33.

252 European Parliament "Texts Adopted".

253 *Ibid*.

254 European Commission "Proposal for a Directive of the European Parliament and of The Council on Liability for Defective Products" https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0495 (accessed 04-05-2024).

255 PLD note 51: "In recognition of manufacturers' responsibilities under Union law for the safety of products throughout their lifecycle, such as under Regulation (EU) 2017/745 of the European Parliament and of the Council16, manufacturers should also not be exempted from liability for damage caused by their defective products when the defectiveness results from their failure to supply the software security updates or upgrades that are necessary to address those products' vulnerabilities in response to evolving cybersecurity risks. Such liability should not apply where the supply or installation of such software is beyond the manufacturer's control, for example, where the product owner does not install an update or upgrade supplied to ensure or maintain the product's safety level. This Directive does not impose any obligation to provide updates or upgrades for a product."

that products can still be within a manufacturer's control after being placed on the market.[256] This means that AI system providers will not be able to rely on this defense if the AI system's defectiveness is due to a particular aspect of the product that remained within their control, including the provision of software updates, upgrades, or any substantial modifications.

Where it has been established that a product is defective and the damage that occurred is, based primarily on similar cases, typically caused by the defectiveness in question, the claimant should not be required to prove the causal link, and its existence should be presumed.[257]

Given that products become superseded and higher safety standards are developed as EDT progresses, it would not be reasonable to hold manufacturers liable for an unlimited period for the defectiveness of their products.[258] Therefore, liability should be subject to a reasonable time, namely ten years from placing a product on the market (the "expiry period"),[259] without prejudice to claims pending in legal proceedings. To avoid unreasonably denying the possibility of compensation for damage caused by a defective product, the expiry period should be extended to 25 years in cases where the symptoms of a personal injury are, according to medical evidence, slow to emerge.[260] The injured party has a prescription period of three years, within which proceedings need to be initiated. The period shall run from the day the injured person became aware, or should reasonably have become aware, of all of the damage, defectiveness, and the identity of the relevant parties that can be held liable for that damage under Article 8.[261]

6 3 AI Liability Directive

Before the AILD, national liability rules based on fault were not suited to handling liability claims for damage caused by EDT-enabled products and services. Under such regulations, victims must prove a wrongful action or omission by someone who caused the damage. The specific characteristics of EDT, including complexity, autonomy, and opacity, make it difficult or prohibitively expensive for victims to identify the liable person and prove the requirements for a successful liability claim.

Specifically, when claiming compensation, victims could incur high up-front costs and face significantly longer legal proceedings than cases not involving EDT.

This caused legal uncertainty. Businesses would have difficulties predicting how the liability rules would be applied, thus assessing and ensuring their liability exposure. It would particularly affect businesses trading across borders and small and medium-sized enterprises (SMEs), which cannot rely on in-house legal expertise or capital reserves.

Under this proposal, the EU Commission addressed an injured party's ability to take non-contractual, fault-based claims in member states. The AILD also complements the AI Act. It introduces a liability regime that ensures legal certainty, enhances consumer trust in AI, and assists consumers' liability claims. The AI Act introduces requirements intended to reduce risks to safety and fundamental rights. Other EU law instruments regulate general and sectoral rules applicable to EDT products. While such provisions are designed to minimise risks to safety and fundamental rights and prevent, monitor, and address societal concerns, they do not provide individual relief to those suffering damage caused by EDT.[262] The effect of the AILD is that it

256 PLD note 59.

257 PLD note 47.

258 European Parliament "Texts Adopted".

259 PLD Art 17

260 PLD note 57.

261 PLD Art 16.

262 "The Artificial Intelligence Liability Directive" https://ai-liability-directive.com/ (accessed 04-05-2024).

will be easier for parties to take non-contractual fault-based claims.[263]

The AILD is limited to claims by parties where damage was either (i) caused by an AI system or (ii) caused by the failure of an AI system to produce a specific output. Its definitions and enactment dates are aligned with the AI Act to ensure consistency. The AILD comprises two critical procedural devices.[264]

The first relates to the ability of injured parties to access relevant evidence.[265] Thus, the AILD follows a minimum harmonisation approach. In the case of high-risk AI systems suspected of causing damage, claimants may request national courts to order the disclosure or preservation of evidence from relevant parties. For high-risk AI systems, the AI Act provides for specific documentation, information, and logging requirements but does not provide a right to the injured person to access that information.

Therefore, it is appropriate to lay down rules on disclosing relevant evidence by those who have it at their disposal to establish liability.

Such disclosure should only be ordered where the potential claimant presents facts and information sufficient to support the plausibility of a claim for damages, they made a prior request to the provider, the person subject to the obligations of a provider or the user, to disclose such evidence at their disposal about specific high-risk AI systems suspected of having caused damage, which has been refused.[266]

Ordering disclosure should lead to a reduction of unnecessary litigation and avoid costs for the possible litigants caused by claims that are unjustified or likely to be unsuccessful. There could be situations where the evidence relevant to the case is held by entities that would not be parties to the claim for damages but are obliged to document or record such proof according to the AI Act. It is thus necessary to provide for the conditions under which such third parties to the claim can be ordered to disclose the relevant evidence. Parties that do not comply are subject to a presumption of non-compliance, facilitating a more straightforward process for the claimant and encouraging relevant parties to comply with the orders.[267]

The second procedural change that the AILD introduces will make it easier to prove a causal link between a relevant party's fault and an AI system's output by introducing a series of rebuttable

263 Launders "Beyond the AI Act".

264 Launders "Beyond the AI Act".

265 AILD Art 3.

266 By limiting the obligation to disclose or preserve necessary and proportionate evidence, Art 3(4), first subparagraph, aims to ensure proportionality in disclosing evidence, i.e., limiting the disclosure to the necessary minimum and preventing blanket requests. The second and third subparagraphs of Art 3(4) aim to strike a balance between the claimant's rights and the need to ensure that such disclosure would be subject to safeguards to protect the legitimate interests of all parties concerned, such as trade secrets or confidential information.

267 Launders "Beyond the AI Act". AILD Art 3(5).

presumptions.[268]

These rules give injured parties a procedural advantage in proving their case. However, they will still have to prove all the relevant substantive criteria of their claim under the laws of each member state.

7 CONCLUSION

Given that EDT is rapidly transforming, much research and development is still ahead of us. The primary concerns raised in this article are that a delict is committed by a human per definition and not by EDT; EDT is complex, and numerous stakeholders are involved in EDT production. We can, therefore, easily understand why EDT-related liability has become one of the main areas of concern for many experts today.

Establishing liability for damages caused by EDT used to be rather candid when only one or a few stakeholders were involved or when the EDT could only take a limited range of predefined decisions following specific parameters defined by a human programmer.[269] However, EDT in the 4IR and future involves several stakeholders and components, making it challenging to allocate liability to all stakeholders. Moreover, recent forms of EDT are increasingly able to learn without human supervision and control, resulting in the ability to make autonomous decisions, which poses tremendous challenges for addressing questions of liability.[270] Indeed, no jurisdiction has granted EDT legal personality to date, meaning that EDT cannot be held liable for the damage it causes as an "electronic person".

Given that EDT is not regulated in South Africa, the most suitable forms of civil liability were explored: product liability, vicarious liability, and the *actio de pauperie*. It was found that product liability and vicarious liability are not suitable for EDT delicts. However, the *actio de pauperie* doctrine might be considered should it be possible to find EDT akin to domestic animals.

The EU has, however, set the bar for regulating EDT. The EU evaluated its product liability regulations, focusing on their continued effectiveness and relevance to EDT. The evaluation process included a preliminary assessment of the continued relevance of the concepts of product liability, such as product, producer, defect, damage, and the burden of proof.[271] The EU now has a product liability framework for products and a more specific legal framework for all stakeholders, which provides a more efficient strict liability context in these cases. The AI Act,

268 AILD Art 4: "Subject to the requirements laid down in this Article, national courts shall presume, for the purposes of applying liability rules to a claim for damages, the causal link between the fault of the defendant and the output produced by the AI system or the failure of the AI system to produce an output, where all of the following conditions are met:
(a) the claimant has demonstrated or the court has presumed pursuant to Article 3(5), the fault of the defendant, or of a person for whose behaviour the defendant is responsible, consisting in the non-compliance with a duty of care laid down in Union or national law directly intended to protect against the damage that occurred;
(b) it can be considered reasonably likely, based on the circumstances of the case, that the fault has influenced the output produced by the AI system or the failure of the AI system to produce an output;
(c) the claimant has demonstrated that the output produced by the AI system or the failure of the AI system to produce an output gave rise to the damage."

269 Benhamou and Ferland "Artificial Intelligence & Damages: Assessing Liability and Calculating the Damages (February 8, 2020). Leading Legal Disruption: Artificial Intelligence and a Toolkit for Lawyers and the Law, Forthcoming" https://ssrn.com/abstract=3535387 (accessed 10-05-2024).

270 *Ibid.*

271 Regulation (EU) No 540/2014 of the European Parliament and of the Council of 16 April 2014 on the sound level of motor vehicles and of replacement silencing systems and amending Directive 2007/46/EC and repealing Directive 70/157/EEC (OJ L 158, 27.5.2014) 131–195.

the PLD, and the AILD accomplish this.

Much work remains to be done in South Africa — not only via legal research but also on the policy, technical, and business sides — before we, as humans, can satisfactorily answer all questions related to EDT civil liability. Because no specific legal regimes currently define or regulate the operation of EDT in South Africa, courts dealing with these questions must attempt to solve liability issues by applying general laws drafted years before the advent of this technology. It is suggested that the EU product liability jurisprudence be followed.