OBSERVATIONS & RECOMMENDATIONS

v20210805

regarding the Proposal (dated 21 April 2021) for a Regulation of the European Parliament and of the Council laying down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts

I. INTRODUCTION

About Arthur Strategies & Systems

1. Arthur Strategies & Systems is part of Arthur's Legal. It has handpicked experienced interdisciplinary experts to focus on ability to navigate, enable, facilitate as well as execute and systemize. Our core team consists of attorneys at law, senior legal counsels, governmental advisors, strategists, innovation, policy & standardisation experts, community & competence builders, all well-connected in the world of human values, societal values, ecological values and economical values, as well as related technology, strategy, ethics, policy, legal matters & global business.

2. Our daily domains are, among others, helping to create, design, architect, build, deploy, succeed and sustain human-centric 21st century cyber-physical and other digital ecosystems, societal challenges, data strategies, trusted data sharing, safety, cybersecurity, privacy, sustainability, transparency, trust, IoT, robotics, autonomous systems, AI, RPA, cognitive systems, attributed- and other evidence-based trust and trustworthiness, human-centric digital transformation, combinatoric applied innovation, competence and capability building, impact-based deployments, resilience, human values, accountability and dynamic assurance. We are already active in most these domains for over 20 years. We are member of the AI Alliance, consortium partner to projects such as STAR-AI.eu, AI4PublicPolicy.eu, ASCAPE-project.eu and CONCORDIA-h2020.eu, and advisory board member to projects such as h2020-AVENUE.eu and many others.

3. As always, we provide our inputs fully independently, where we are aiming for building human-centric and future-proof ecosystems that are addressing societal challenges while being transparent, trustworthy, transformative yet inclusive, and where all stakeholders are accountable and co-accountable, for people, planet, prosperity, peace and partnership.

We Support & Endorse

4. We welcome the opportunity to provide our observations and recommendations. We strongly support and endorse the initiative by the European Commission for the current proposed Artificial Intelligence Act[1]. We find it a very impressive (draft) act already. This initiative will help ensure that AI is safe, lawful and in line with EU fundamental rights, and related accountability (and liability) attribution.

[1] EU Commission (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. COM(2021) 206 final, 21 April 2021: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12527-Artificial-intelligence-ethical-andlegalrequirements_en

5. The overall goal is to stimulate the uptake of trustworthy and accountable AI in EU society and economy. We underline the importance of establishing such framework to foster safe, trustworthy and accountable AI-supported innovation while addressing Societal Challenges.

6. We also strongly support the proportionate, risk-based approach. Adding AI to a process, technology or (eco)system could strengthen the capacity to do good, in an accountable way, and address societal challenges – of which also the EU and its member states, communities and citizens have plenty, both short term, mid term, long term and extreme long term –,

   However, adding AI to the equation also can increase risk, and augment or trigger potential material detrimental impact. It is important to ensure that these risks are mitigated, and organisations (whether providers, users or otherwise) are held ethically, socially and legally responsible, accountable and liable.

7. We believe that the current proposed AI Act is generally well-developed; however, some parts are not yet sufficiently developed or otherwise deserve further considerations, conditions, qualifications, detailing and other improvements.

II. OBSERVATIONS & RECOMMENDATIONS

Multiplicity; human (value) centric

1. Digital technology, climate, pandemics, and other dynamic changes the world at a fast pace. Yet, humans are underrated. Build, enhance and retain trust with the combination of human brain power, purpose & passion, machines, algorithms, data and accountability.

   We always aim for the human-centric, trusted and trustworthy Multiplicity Approach: a certain, dynamic symbiotic combination of diverse groups of people with diverse gender and diverse backgrounds that work together with diverse groups of human-centric machines, algorithms and capabilities to identify, address and solve problems, make and – where appropriate – execute decisions, and double-looping capabilities to never stop learning.

   Technology has outstripped the (universal) human values, societal, economical and legal frameworks; how to catch up, and keep up?

2. Most of the particular domains, risk areas and other dimensions that the proposed Artificial Intelligence Act focuses on, can also happen, be met or achieved (or impacted, either positively or negatively) without the use of AI – as defined in the proposed AI Act in general and its Annexes in particular. It is very good to use a technology domain such as AI as a use case and scenario plotting and mapping catalyst, in order to identify, classify and address the various additional risks (either new, combined, augmented or otherwise).

   However, this will not address, mitigate or solve the challenges that existing data analytics, algorithms, software, computing, platforms and other technology can already provide, closely mimick AI capabilities (regarding functionality and outcomes).

3. The focus on AI therefore is good for purposes of this proposed AI Act, but let's not forget the many other technical layers, systems, products, services, convergence thereof and related opportunities and challenges that AI aimes to address, and risks that are either already happening, accruing, evolving, emerging (and creating problems including concentration risks) every single day.

4. Our conventional ways to organise and govern those are too slow to catch up and keep up. The instruments we deploy (paper versus digital) also are not sufficient enough in this 21st Century – noting that we are already for 21% in that century –. Digital policy instruments to help keep AI and other technology and digital ecosystem transparent, trustworthy and under meaningful control with clear (timely) accountability should be part of the equation. Diverting, mandating or otherwise referring enforcement and the like to member states and public sector organisations in the traditional way means: (public sector on behalf of the) people versus digital. That has already for at least 15 years been proven an unequal match where people (and the citizens, societies, economies – and our planet – that depend on swift, proper and clear enforcement, redress and remedies) lose. This needs to be taken into account when trying to rule, govern, control, monitor and otherwise organise AI and AI systems, whether high risk or not. For once, a principle-based, technology-neutral, dynamic, hybrid and lean approach is one of the main success factors.

Holistic Involvement & Approach

5. As mentioned in the proposed AI Act, the definition of 'AI system' aims to be as technology neutral and future proof as possible, taking into account the fast technological and market developments related to AI. We appreciate that, as mentioned above, although the AI Act is one of the least technology neutral EU regulations of the past 7 years.

6. Artificial intelligence (AI) supports, as a mere tool – and, when designed, deployed and maintained well – a great tool, next to the many others. AI is not a separate, stand-alone technology that makes everything happen. Focusing too much on anything means staring at one thing, and also in this Digital Age this means one misses everything else (and the point).

7. Furthermore, artificial intelligence systems, or better: artificial intelligence-supported systems ('AI systems') are way more than part of the software layer. It can be part of a services; it can be part of ecosystems of systems. These (eco)systems are converging, meaning that verticals merge, submerge and otherwise integrate into other sectors, markets and domains – whether new or not AI can also be part of a backend system; so not marketed in that sense, but still highly impactful to people, health and fundamental rights. As mentioned above already as well, a very small piece of AI capabilities in large (eco)systems, placed either upstream, midstream or downstream, can have potential high value, but also high risks. It is quite contextual.

8. In any case, it is essential to have a horizontal, cross-cutting and cross-sector approach. AI will almost never be a stand-alone technology. It will be part of one or multiple technical stacks, in one or multiple sectors, markets and domains, and these are not isolated or otherwise silo-ed.

9. As per the ongoing convergence these are becoming more and more connected, interconnected and hyperconnected, bringing greater opportunities and cross-fertilization, but on the other end also can infect and affect each other easily, and augment known and unknown threats, vulnerabilities and other risks. Furthermore, various life-cycle factors need to be considered right from the design phase all the way through the end-of-life phase to ensure transparency, trustworthiness, safety, resilience, accountability, remedies and redress. We believe that it should be set very clear in the AI Act that this all is part of the term AI systems, and in scope of the AI Act.

Intended, Expected & Actual Purpose, and (Actual) Use

10. Where the current proposed AI Act only focuses on 'intended purpose' (which will be defined by the provider, accordance to the current definition in Article 3(12), and the 'reasonable forseeable misuse' (as currently defined in Article 3(13)), also as per the fact that AI systems can be quite extensive and AI functionality may have been defined by the provider as stand-alone where it already knows – or can expect – in advance that it will be actually deployed or otherwise used in an AI system (that, in this example, is not stand-alone), it is not clear enough in the current proposed AI Act whether this is in scope of either 'intended purpose' or 'reasonable forseeable misuse'. One could argue, it falls under the latter (having a formal view that anything that is outside the 'intended purpose' is 'misuse'), but it leads to providers defining the 'intended purpose' extremely narrow, where the provider knows the expected use as well as the actual use is (far) outside such narrow definition. This for instance could lead to defining the intended purpose to a non-high-risk purpose where it is well-known it will be used in a high risk environment.

11. Defined intended use versus the real, complex and already and ever increasing connected, interconnected and hyperconnected worlds and ecosystems balances out to a win for the definition (and another loss for people, society and others), if this is kept too rule-based and not principle-based. This, is a lawyer's paradise, and although Arthur's Legal is a law firm as well, we are very keen and determined to avoid this, and further optimize policy instruments – such as the proposed AI Act – where and when we can.

12. A classification of various abstract purposes and use can be:

    a. intended purpose
    b. intended purpose is also the expected purpose/use
    c. intended purpose is also the expected purpose but not the actual purpose/use
    d. intended purpose, but not the expected purpose/use
    e. intended purpose, but not expected and actual purpose/use
    f. unintended use
    g. unintended but expected purpose/use
    h. unintended but expected purpose and actual purpose/use, or
    i. unintended and unexpected purpose
    j. unintended, unexpected yet actual purpose/use.

13. Insights in risks, whether high or otherwise, do not merely result from the intended purpose, as these only reveal hypothetical risks (including levels of probability and levels of impact and consequences). Even more so, risks happen (or can happen or otherwise reveal themselves) from the expected purpose, actual purpose and most importantly, to the actual use; in the real world.

    The main point we are trying to make regarding to focus on intended purpose, is that is to be avoided only to look at 'well-drafted' definitions of what the intended purpose would be. It would be otherwise too easy to avoid being accountable and co-accountable, and push away responsibilities (and liabilities).

    The inclusion of the more subjective and less-manipulable term of 'reasonably foreseeable misuse' already helps a lot but does not cover the relevant purposes set forth above.

Risk (Segmentation) in AI and AI-supported Systems

14. It is important not to percieve risk as always something necessarily negative. It is an integral part of the equation and with that an enabler and facilitator of anything that works in a trusted, trustworthy and accountable way. It gives essential and valuable insights to what may happen or may go wrong, what people or society like or fear, et cetera. For instance, being an entrepreneur or director in the private sector is all about risk-analysis and well-informed decision making. For sure, in the AI or AI-supported domain risk an essential success factor as well.

15. The magnitude of risks, determined by the probability as well as the impact thereof, is very much context and application dependent. To prepare for and mitigate the potential harm, to embed preparedness for foreseen and unforeseen situations, and to make it resilient and future-proof, it is necessary that AI systems are designed and deployed guided by trust principles. These non-functionals are principles that consistently preserve trust, trustworthiness and engagement of all relevant stakeholders, and the currently proposed AI Act already has embedded the most relevant ones, such as security, safety, privacy, accountability and robustness. There are several hundred of these trust principles; to date, our firm has identified almost 500 unique trust principles. These can be found in best practices, guidelines, white papers, standards, regulations but also in common practice and nature.

16. Two major challenges in the AI design and deployment are (1) to map the relevant risks accurately and comprehensively throughout the system's entire lifecycle, and (2) to incorporate non-functionals by design. It is at least useful to segment the various AI-related dimensions of this Digital Age in order to get some relevant oversight and insight.

    For purposes of this (relatively brief) contribution, the initial segmentation is however done in four (4) segments as set forth below:

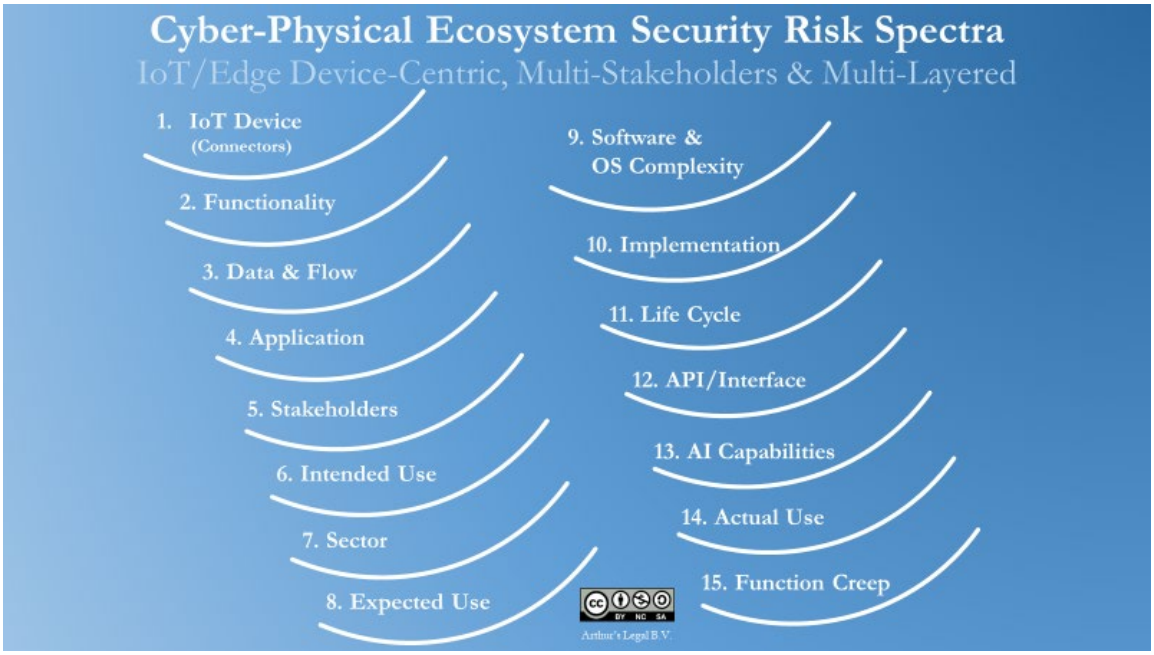
    a. **Non-connected**, which is a stand-alone device, tool, machine, appliance or application that does not have connectors or connectivity that can connect to the internet or other external network or resources.

b. **Connected**, where a device, tool, machine, appliance, application or system may be connected to, via the internet, a centralised databases, cloud infrastructure and other centralised systems;
c. **Inter-connected**, where several edge devices, tools, machines, appliances, applications or systems are connected with each other, either via orchestrated, federated systems, and;
d. **Hyper-connected**, where numerous far edge and other IoT devices, tools, machines, appliances, applications or systems are directly connected with each other via distributed (computing and related) ecosystems of ecosystems.

17. For each of these segments, various value cases, business models, feasibility models and therefore use cases can be identified and created in the AI & AI-supported systems. Each segment has its own values, benefits, efficiencies, inefficiencies, et cetera. The segmentation set above obviously is not the only one possible. Various other segmentations are relevant to consider as well, such as for instance real-time, near-real-time or not. This segmentation may be relevant when near-real-time autonomous 3D printing is considered, or real-time prognostic health monitoring or related integrated logistics support is relevant. Other segmentations that can be considered are single-vendor, multi-vendor, OEM, public, private, public-private, et cetera.

Risk Classification Spectra: A Multi-Layered Approach

18. When going back to the above-mentioned segment, Hyper-Connected devices, and taking a risk-perspective to those, a methodology to do high-level quality risk classification is to have a multi-layered approach and do such risk classification per spectrum, starting with the risk classification of the connectors and connectivity of, for instance an IoT device itself. Even though AI capabilities may not yet be in the equation, it is essential to understand the various risks that are embedded in or could arise from such AI-supported IoT device. Subsequently, other risk spectra should be considered and risk classified, as visualised below.



19. Especially more downstream there may be risk spectra that may not be relevant; however, if such spectrum may become relevant later in the life cycle of the IoT device it is recommendable to keep it in and already do the spectrum risk classification. In general, three categories of main risk levels are used: low, medium and high. Based on the outcome of (i) a risk classification for each spectrum, and (ii) the interim outcome of the various risk classifications up to Spectrum 13 (AI Capabilities), the baseline risk classification can be established.

20. Based on that baseline, the AI Capabilities risk classification can be done, and the subsequent risk spectra; the holistic perspective constitutes the Combined Risk Classification, on which one can consider and organise technical & organisational security, safety, privacy and related technical and organisational measures.

21. Any technical and organisational measures taken or to be taken can include, cause or otherwise trigger risk by itself or as a trigger consequence. It is therefore recommended to double-loop the particular set of measures, for once to initially assess if and to what extent these may have a detrimental impact.

22. As per the dynamics of IoT – and even more so AI-supported IoT and IoT ecosystems – any of the risk classification spectra can be expected to trigger, change or otherwise show relevant dynamics, such as (A) technical or other threats and vulnerabilities, (B) actors and other stakeholders anomalies, updates or upgrades in code, datasets or attributes, or (C) changes in regulatory standards, policies or other relevant best practices, it is recommended to double-loop as well, including those spectra that are or may be related or otherwise are (inter)depended on the particular spectra. Therefore, it is recommended to continuously monitor the risks, and where necessary or otherwise double-loop thereafter to keep the security measures up to date and resilient.

23. In any case, the segments, whether non-connected, connected, inter-connected or hyper-connected, that have AI capabilities of any kind, are for sure game changing, where non-functional and functional requirements have to be addressed together.

Biometrics in the (semi)Public Domain

24. On another topic that is addressed in the currently proposed AI Act and we would like to make an observation and recommendation about, it is not clear why real-time remote biometric identification systems used by private sector organisations in publicly or semi-publicly accessible spaces have not been prohibited (with clear yet strict exceptions). This, as the consequences of misidentification in the case of individual persons can be far-reaching and highly-impactful. Reference is made to the joint EDPB and EDPS Opinion on the AI Act of June 2021[2] which nicely clarifies that the use of these technologies may easily result in 'the end of anonymity in these spaces'.

[2] EDPB-EDPS Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) of 18 June 2021: https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en

Law Enforcement

25. While we have a high level of confidence in the legal systems in each of the member states, including law enforcement, it needs to be – very clear – that law enforcement agencies and related organisations can only use AI or AI-supported remote real time biometric identification systems or similar, in case of a 'serious crime'.

26. Most exceptions in the proposed AI Act seem reasonable, considering their narrowly defined scope, except for the one set forth in Article art. 5.1(d) under iii, as it allows such technologies to be used in the context of an arrest- and surrender order regarding offences to which 'maximum punishments of 3 years or more' can be imposed. This is not a proper threshold for 'serious crime', giving too much room for misinterpretation and potential misuse, and therewith to little factual clarity and legal surety to people, organisations and society.

27. In this context, it is also unclear how non-suspects will be protected against the (mis-)use of biometric systems targeting suspects of serious crimes. Furthermore, it should be questioned how citizens will be protected by use of biometric infrastructure by authorities, that does not align with the fundamental rights under EU law.

Currently Underdeveloped: Market Authority Discretion

28. Similar to the last paragraph, we are concerned about the current structure, qualifications and conditions set forth in Article 67 about compliant AI systems which present a risk. Assuming that one has a highly ethical, safe and trustworthy AI system that is fully compliant to the requirements set forth in the current proposed AI Act. A market authority in a member state can under Article 67 still argue – and as per the current wording quite subjectively and randomly – if it may think such compliant AI system should be withdrawn, recalled or 'corrected'.

29. Next to the question about legal uncertainty and potential random and bias acts and behaviour that can occur (for political, local or national competitive, economical or any other reason), it would lead to the great minds, researches, entrepreneurs and (municipality, regional) leaders and other lead-users in any sector – not – to invest time, money and other resources in the development, marketing, deployment, use and feed-looping of highly ethical and compliant AI systems. This, as the risk that its – expensively design, build and maintained – AI system may be banned without the ability of making prior informed decisions. Therefore, even though most of the proposed AI Act in our view is well-developed, this topic and Article needs to be further developed, and nuanced, also to protect investors, entrepreneurs, providers, users and society.

Facilitating (and Automating) Conformity Assessments for SMEs

30. As one does generally not outsource its own thinking, and not outsource making its own decisions, it can be expected that AI and AI system will be developed and used, by the users themselves.

A director or Chief Executive Officer of a SME, Midcap company or large corporate also does not make the decisions solely itself but jointly with the various board members, staff and experts. Where large corporates may have the capability to do conformity assessments of AI and AI systems itself, for the, also in the EU essential SMEs and Midcap companies, it will probably be too expensive and otherwise burdensome.

31. Therefore, we would recommend that such assessment of AI created, provided or used by SME's are facilitated (for instance through automated assessments or dynamic assurance) or otherwise supported[3]. The same goes for municipalities and other organisations who do generally not have the resources for these efforts.

Private Law Remedies & Redress

32. While the currently proposed Artificial Intelligence Act lists numerous stakeholders and human-centric, the citizens and related organisations are not stakeholder in the current proposed AI Act. There are no direct remedies, redress or similar legal instruments available for the people of the EU themselves. This was also the case in the 1995 Privacy Directive and has been corrected in the current GDPR. It is recommended to provide for legal instruments in the AI Act that EU citizens (either individually or collectively, via an EU legal entity such as a foundation or association or not) can enforce themselves. This, next to the administrative instruments that the current proposed AI Act caters for, to the member states.

III. IN CONCLUSION

33. Especially the past five (5) years, the Commission respectively European Parliament have been consistently taking initiatives in the form of strategies, action plans, legislations and other instruments to both grasp the opportunities of data, technology, and human-centric digital capabilities as well as identify and address the risk and related responsibilities, accountability and liability. This is highly appreciated, also regarding AI and AI(-supported) systems. We are for sure moving in the right direction. Also this initiative could mean leadership of these opportunities and challenges on a – to quite some extent – global scale.

34. The current proposed AI Act is a very impressive regulation. As any other draft/proposal, it does however need some further considerations, improvements and other optimisation, including the ones related to the observations and recommendations set forth in this document.

35. While doing that, it is important to have a holistic approach, both from perspectives of ecosystems of systems, society, communities and economies it can influence, impact, manipulate, lead, steer and otherwise affect (both positively, negatively and from a net-benefit point of view), as well as life-cycles. This, to ensure that one does not view AI and AI systems in a linear and stand-alone manner but instead in a holistic and future-proof manner.

[3] Currently proposed Artificial Intelligence Act, Articles 19, 26 and 43

36. We believe that our – limited and not exhaustive – observations and recommendations mentioned above support the Commission in its mission to successfully develop and later on passes a high-quality and highly-impressive and positively impactful AI Act. There is no denying that the EU has been a front-runner in ensuring that the different facets pertaining to the human-centric digital domains are regulated with introduction of the General Data Protection Regulation, ePrivacy Directive, Regulation on the Free Flow of Data, NIS Directive, Cybersecurity Act, and upcoming regulations and directives in this Digital Age.

37. We continue to be dedicated to this and are as always ready to further help and engage and keen to further elaborate on the above at the Commission's request.

Amsterdam, 5 August 2021 / Arthur's Legal, Strategies & Systems