Discover Artificial Intelligence

Discover

Comment

Should we regulate Artificial Intelligence or some uses of software?

Joshua Ellul[1,2]

Received: 13 February 2022 / Accepted: 1 March 2022
Published online: 08 March 2022

Abstract
Artificial Intelligence regulatory developments have been ever-increasing in both academia as well as within policy and governmental settings. Whilst extensive literature has been published on the topic of how such regulation should be developed, the question as to whether such regulation should be AI-specific or focused on software in general remains unexplored. In this commentary paper this question is explored and after arguments for whether regulation should be technology-specific or be focused on the use of technology are provided.

Keywords Artificial Intelligence · Regulation

1 Introduction

Artificial Intelligence (AI) is without a doubt becoming an integral part of our daily lives—from its pervasive use in social media, to search engines, home appliances, and beyond. 'Regulation of AI' has been a hot topic over the last decade, and it is no surprise considering both its current and future potential impact on society. Many have proposed the need and ways to regulate the use of AI in the context of social media platforms [1], health systems [2], autonomous vehicles [3], finance [4], amongst other sectors and activities. Recently the EU laid down a proposal for AI-specific regulation (EU's draft AI Act)[1] which has received varying feedback [5–7]. In this commentary, a discussion is presented pertaining to two pertinent questions: if we should regulate AI, (i) what should we regulate? Should we be regulating AI or software in general? and (ii) where should we regulate? should we be regulating the technology at large or specific use of the technology?

Indeed, the question of whether we should regulate technology/software/AI at all or just ensure that legislation is technology neutral and enforces desired principles (e.g. non-discrimination) is a pertinent one. However, this question deserves a paper in its own right. In this paper, we assume that there exists some form of need for regulation for some use of AI/software—for example systems used in a safety-critical setting must undergo proportionate scrutiny to ensure their adequateness. Such regulation could take place as hard-laws, regulatory guidelines or other. In this paper we do not delve into such specificities yet focus on the questions laid out above.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

✉ Joshua Ellul, joshua.ellul@um.edu.mt | [1]Malta Digital Innovation Authority, Mriehel, Malta. [2]Department of Computer Science, University of Malta, Msida, Malta.

2 Varying degrees of regulation

Regulation can come in many shapes and forms, and an associated wide spectrum of opinions in regards to what type of regulation, if any, should be applied to AI. From advocating for mandatory AI regulation [8], to voluntary certification [9], soft and self-regulation [10], the need for explainable [11] and ethical frameworks [12], and standards [13], hybrids thereof, and that AI should have complete freedom requiring no form of regulation.[2] Whichever school of thought one subscribes to (even for one that promotes development completely free of regulation), it is reasonable to believe that one would prefer to board a plane that has undergone high levels of assurance processes and safety-checks—which are a form of regulation. The same would go for a plane controlled by AI. Naturally one would also prefer to board a plane for which its AI has also undergone sufficient quality controls, assurances, testing, and functional correctness checks. So, in the very least, there should be agreement that there exists some form or instance of AI-based systems that should undergo some form of regulation. It is not the purpose of this paper to delve into what level of regulation should be applied and how it should be applied (as extensive literature delves into this detail), yet only to discuss the questions previously laid out. Having established that there exists some form or instance of an AI-based system that should be regulated to some extent, the questions laid out will be discussed.

3 Regulate AI or software?

Irrespective of the type of regulation that should be opted for, should AI specific regulation be posed or should regulation be algorithm-agnostic? Firstly, one would need to define what AI is (and/or what it is not) so as to ensure that only systems that should be classified as AI fall under regulation—and that systems that should not be classified do not.

What AI is and the definition of AI are topics that have been debated and discussed for decades [14–19]. Until a universal definition of AI is proposed that includes all systems that should be classified as AI and does not include systems that shouldn't, such a legal system would create regulatory gaps and uncertainty with respect to what falls within regulation. Also, such a definition risks capturing within it systems that should not be captured, and/or not including systems that should be. More so, such gaps would allow developers to avoid such regulation by ensuring their implementation falls outside the posed definition of AI.

Proposals have been made to, rather than define AI, describe features of AI-based systems as a means of determining when a system should be classified (or not) as AI [18, 20]. In fact, the EU draft AI Act proposes to define AI in such a manner. Yet, rightly so, due to future potential development it states 'which should be kept up-to-date in the light of market and technological developments'.[3] If such a means of defining AI is adopted, given the fast pace of technological development, it would be crucial to question whether laws could be updated sufficiently fast enough to ensure that technologies cannot escape the law for a period that is long enough to cause substantial negative consequences. Given these risks, one should question whether a definition of AI is required at all, or whether the focus should be on software in general. Mandatory software regulation is not being advocated for here, but that wherever it is deemed to be required, regulation should be focused on software and not be AI-specific (though guidelines on how to provide adequate assurances for specific technologies such as AI would be beneficial). Indeed, in the case of critical software used in a plane, whether AI is used or not is irrelevant.

Secondly, assuming that one does not see the above as enough justification as to why regulation should not be AI specific, consider the use-case of AI used in banking or insurance systems that decide whether or not a particular loan or policy should be offered. Regulation should aim to ensure that clients are not discriminated against. Should such regulation apply only to AI-based systems? One could code a system to make decisions using non-AI techniques. Should such a system not be required to undergo proportionate levels of scrutiny to ensure its adequateness to make such decisions?[4] If only AI systems are captured within such regulation, then the specific regulation would not be able to ensure that

[2] https://www.technologyreview.com/2017/10/24/3937/dont-let-regulators-ruin-ai/.

[3] See (6) of the Proposal for 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. Explanatory Memorandum. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[4] We could also go a step further and question whether such regulation should be independent of who or what the decision maker is, i.e. if the decision is made by a human, should the same scrutiny not be applied to associated processes?

all digital systems used in such contexts are adequate to make such decisions. The same argument applies to all other use-cases where regulation is deemed to be necessary. Of course, how one reaches the levels of assurances required for different technologies may differ (e.g. AI systems typically require beyond functional correctness checks to also ensure that training data is sufficient)—however that is besides the point. Based on this, **regulation should not be AI specific but should be wider on software in general** (while guidelines on how to provide assurances indeed should factor different challenges that different technologies pose).

An alternative would be to provide a definition of AI that is all encompassing, including all types of software, automated, and digital systems. However, whilst no universally accepted definition of AI exists, the term has been used by computer scientists, engineers and practitioners for decades to define algorithms that use certain techniques and/or exhibit certain features. Whilst a solution could be to widen the term AI to be all encompassing and include software, this would be counter productive. Since individuals and entities operating outside the AI sector and those that are certain that they do not make use of AI would likely not concern themselves with 'AI'-specific regulation—and why should they?

3.1 Would software regulation result in loss of focus?

One might question whether wider software regulation, rather than more specific AI regulation, shifts the focus to be too far away from features that are typical of AI systems including 'opacity, complexity, dependency on data, and autonomous behaviour'.[5] Indeed, it is the case that wider regulation may result in diluting focus—and we should question the potential impact of this. Let's consider the defining features listed above from the EU draft AI Act.

Whilst, AI-based systems more often tend to exhibit 'opacity, complexity, dependency on data, and autonomous behaviour', such features are not exclusively associated with AI. Many AI algorithms are inherently opaque yet are not intended to be opaque by design. In fact, extensive effort is being undertaken towards enabling them to be more transparent. At the same time, there are classes of algorithms that are intended to be opaque by design so as to: not leak sensitive information [21], preserve privacy across multi-party computation [22], and protect software IP [23]. If software process/data opacity is a concern when considering particular applications (e.g. bank loan processing), then surely it should be a concern irrespective of whether the associated algorithm is AI-based or not, and whether opacity is built into the algorithm by design or not.

Over the past decades software systems have grown to become ever increasingly more complex, often built from myriads of components to produce a single-system comprised of many distributed computing systems working independently. As software systems in general (that do not necessarily make use of AI) 'grow in complexity, interconnectedness and geographic distribution, we will increasingly face unwanted emergent behavior' [24]. Indeed, AI algorithms may further introduce an added layer of complexity, yet the high degree of interconnectedness of modern day computational systems make them complex in and of themselves. Therefore, the argument for the need for assurances when it comes to complexity and emergent behaviour is not isolated to AI-based systems themselves.

Many types of AI algorithms are dependent on external data in aim of identifying patterns and trends to be able to make future predictions that may match or follow identified patterns or trends. Again, data dependency is not a feature that is limited to AI algorithms. Big Data techniques such as MapReduce are completely dependent on data—large volumes and variety of data generated at high velocity.[6] Whilst Big Data and AI algorithms are complementary [25], Big Data techniques can also be used in isolation without AI-based techniques—and if algorithmic dependency of data is a feature that (in some applications) is deemed to require some form of oversight then such applications should not be able to escape oversight just by using non-AI techniques.

What autonomy exactly means differs according to the application and object of autonomy. However, in its simplest form, 'autonomous simply refers to the ability of a machine to operate for a period of time without a human operator' [26]. Indeed, many autonomous systems we refer to nowadays are likely to make use of some form of AI though not all necessarily do. Whilst at the same time many other non-AI-based automated systems would also fall under this definition of autonomy. However, it is not a definition of autonomy that should be the deciding factor in regards to whether or not activities or systems should follow regulatory requirements—but system behaviour that should warrant regulatory oversight. Looking specifically at EU's draft AI Act there is clear concern regarding

[5] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

[6] Big data is now typically characterised by 5 Vs rather than just the 3 Vs mentioned.

actions based on decisions made by algorithms, and emphasis is made so as to ensure humans are kept in the loop. However, such decisions need not necessarily rely on AI algorithms and could be made using non-AI algorithms. The key behaviours here are that of automated and autonomous actions, for which non-AI-based systems can also exhibit. Furthermore, autonomy raises questions and concerns of agency, for example regarding copyright. When an autonomous AI application creates an art piece it is hard to determine who the creator is [27, 28]. Whilst, the use of an AI algorithm makes determining this much harder, the same problem exists for software making use of non-AI-based algorithms that may exhibit similar behaviours. For example consider an autonomous non-AI algorithm that generates art pieces based on a random number generator—add to the mix as well other external data or phenomenon that result in manipulating the generated art piece (for example the amount of time it takes for a popular website to reply back to a request for a particular URL).

The points above demonstrate that certain software systems will also exhibit behaviours similar to that often associated with AI-based systems, and are also of concern when considering activities or sectors that deem regulatory oversight. The focus is not diluted, yet in fact it remains the same. What may differ is how to provide assurances for the different techniques, but these are solutions that should not necessarily be prescribed by law (but potentially through technology specific guidelines).

More so, quantum computing will drastically change what can be achieved using computational devices. Problems that now take an infeasible number of years to solve with traditional computing, could take a negligible amount of time to solve using quantum computing—and certain applications of AI and machine learning could be replaced using quantum computing [29]. Such solutions may involve brute-force computation that evaluates every possible outcome to find the/an optimal solution. An algorithm that exhaustively explores a search space is most definitely not AI (at least not through a traditional view of AI). Should such algorithms and systems be able to escape such regulation? Surely not. By regulating software, rather than AI, not only can focus remain on the behaviours that many particularly associate with AI, but regulation can be technology agnostic and focus on behaviours and outcomes rather than technology-specifics (which will become quickly outdated). Furthermore, it is these specific behaviours of concern that should be focused on (rather than AI).

4 Regulate all or regulate only where required?

Whether one comes to the conclusion that regulation should be AI-specific or not, a pertinent question that needs to be asked is whether the technology should be regulated across the board or whether regulation should focus on specific use of the technology. If we were to regulate AI, should all AI be regulated or should it only be regulated when used in certain contexts?

Just like software is the engine that drives the process it is being used for, engines and motors drive the cars, vehicles and planes they are installed in. We do not regulate motors and engines, but we regulate transport and aviation—i.e. the sector/activity. If one were to regulate all motors and engines, then this would include types of motors and engines that would not make sense to regulate, including those used in hard drives, electric wrist watches, and others. Of course, better justification than just this is needed, however the analogy is posed to help differentiate between the technology and the sector/activity. Aviation will continue to be used as a running use-case—indeed the aviation sector is regulated, and already does impose technology based requirements and processes.

Above in Sect. 2 we made a case to demonstrate that regulation is definitely required for some instances of AI/software (e.g. when used in aviation). Yet, should all AI/software be regulated? Should your calendar scheduling software be regulated anymore than what existing laws require of it (e.g. privacy law, consumer law, etc.)? Say it includes AI—should it be regulated just because of that? Consider an AI-based chess bot—should it be regulated? Do the benefits (if any for these use-cases) outweigh regulatory/compliance overheads introduced? Especially when considering the potential impact on AI-based innovation?

Furthermore, it is important to understand what AI is/isn't to answer this question, and without having a deep understanding of AI, it would be presumptuous to attempt to pose regulation. AI is software. Software that has particular features, exposes particular behaviours or uses particular techniques which most computer scientists would more or less agree upon (with some variation). Some AI techniques use nothing more than statistics and probability—e.g. based

on historical data and experience, future predictions can be made. Are we posing to regulate statistics? Clearly not. However, would it be suitable to regulate aviation processes that make use of statistical/probabilistic software (or AI)? Definitely. **Regulation should be applied only where it is required**.

5 Should mandated regulation be technology focused or sector/activity-specific?

If one agrees that regulation should be required based on where it is applied, then the question to ask would then be whether (i) technology-specific regulation should be posed that mandates in what contexts such regulation takes effect or (ii) whether sector/activity specific regulation should be updated where required or posed if needed to mandate such regulation.

EU's draft AI Act takes the first approach above with AI-specific regulation. Let's ignore that it is AI-specific and consider regulation focusing on software systems (since the AI vs software systems debate was discussed in Sect. 3). The draft act provides exclusions for some uses[7] of AI.[8] Thereafter, a risk based approach is used to determine the level of regulation. Such a risk-based approach allows for adequate regulation to be applied where necessary so as to both protect consumers and the market as well as to support innovation. The trade-off for a technology-wide risk-based approach is that determining an application's risk level on all systems may impose overheads on systems that would clearly not require regulation, and that it may result in duplication of laws where such regulation is already imposed on technological solutions (whether directly or indirectly).

The alternative would be to mandate such technology regulation through sectorial and activity focused regulation. For example aviation, other safety-critical areas, and data protection and privacy laws could mandate technology focused regulation (e.g. only mandate something like EU's AI Act where other sectorial/activity laws require). Technology-focused regulation, rules and guidelines could be put in place so as to ensure standardisation across sectors, yet should not be mandated unless stated by other sectorial or activity focused laws and regulation. Such an approach would only require sectors or activities deemed to require such regulation to carry the burden of regulation (indeed a risk based-approach should nonetheless be used). The trade-off to this approach is that it involves more national/supranational legal changes and stakeholder involvement, however it does not suffer from capturing within it all systems.

6 Conclusions

Discussions and policy surrounding AI regulation are steaming ahead, and we have even seen draft AI laws proposed. But did we jump the gun and focus on AI hastily without considering whether such regulation should be focused on AI or whether it should be algorithm agnostic? Based on the discussion presented through this paper, it seems so. It is not too late for EU's draft AI Act to ensure that regulation is algorithm agnostic and does not suffer from pitfalls discussed herein (though it would likely need a new title). Many other questions remain in regards to how to go about such regulation, but we leave such questions for future work.

To summarise, in this paper, two main questions relating to AI (and software/technology) and their regulation were investigated: whether such regulation should be AI-specific, or if it should be wider on software in general; and whether regulation should primarily be mandated in a technology-focused or sector/activity-specific manner. In doing so, it was posed that: (i) regulation should not be defined around 'Artificial Intelligence' but should be wider for software in general; and (ii) regulation should not be applied across the board but should only be mandated where required. A conclusion with respect to whether technology regulation should be mandated through technology-specific laws or through sector/activity-specific laws was not reached, yet arguments for the both sides of the argument were provided.

[7] Military, use by authorities and others.

[8] Here we do not go into the merits of which specific use cases should/not be excluded as that is a different question.

Authors' contributions JE wrote and reviewed the main manuscript text. The author read and approved the final manuscript.

Declarations

Competing interests Whilst only a minor competing interest, the work and view presented in the paper indeed are influenced by the way regulatory frameworks have so far been implemented at the MDIA. That being said, MDIA would need to adopt any policy imposed on it by EU.

References

1. Sivek SC. Social media under social control: regulating social media and the future of socialization. Electron News. 2010;4(3):146–64.
2. O'Sullivan S, Nevejans N, Allen C, Blyth A, Leonard S, Pagallo U, Holzinger K, Holzinger A, Sajid MI, Ashrafian H. Legal, regulatory, and ethical frameworks for development of standards in artificial intelligence (AI) and autonomous robotic surgery. Int J Med Robot Comput Assist Surg. 2019;15(1):1968.
3. Carp JA. Autonomous vehicles: problems and principles for future regulation. Univ Pa J Law Public Aff. 2018;4(1):5.
4. Lightbourne J. Algorithms & fiduciaries: existing and proposed regulatory approaches to artificially intelligent financial planners. Duke Law J. 2017;67(3):651–79.
5. Ebers M, Hoch VR, Rosenkranz F, Ruschemeier H, Steinrötter B. The European commission's proposal for an artificial intelligence act—a critical assessment by members of the robotics and AI law society (RAILS). J. 2021;4(4):589–603.
6. Veale M, Borgesius FZ. Demystifying the draft EU artificial intelligence act—analysing the good, the bad, and the unclear elements of the proposed approach. Comput Law Rev Int. 2021;22(4):97–112.
7. Kiseleva A. Comments on the EU proposal for the artificial intelligence act. SSRN 3949585. 2021.
8. Smuha NA. From a 'race to AI' to a 'race to AI regulation': regulatory competition for artificial intelligence. Law Innov Technol. 2021;13(1):57–84.
9. Ellul J, Pace G, McCarthy S, Sammut T, Brockdorff J, Scerri M. Regulating artificial intelligence: a technology regulator's perspective. In: Proceedings of the eighteenth international conference on artificial intelligence and law. 2021. p. 190–4.
10. Erdélyi OJ, Goldsmith J. Regulating artificial intelligence: proposal for a global solution. In: Proceedings of the 2018 AAAI/ACM conference on AI, ethics, and society. 2018. p. 95–101.
11. Hamon R, Junklewitz H, Sanchez I, Malgieri G, De Hert P. Bridging the gap between AI and explainability in the GDPR: towards trustworthiness-by-design in automated decision-making. IEEE Comput Intell Mag. 2022;17(1):72–85.
12. Wagner B. Ethics as an escape from regulation: from ethics-washing to ethics-shopping. In: Being profiling: cogitas ergo sum. Amsterdam: Amsterdam University Press; 2018. p. 86–90.
13. Zielke T. Is artificial intelligence ready for standardization? In: European conference on software process improvement. Springer; 2020. p. 259–74.
14. Lehman-Wilzig SN. Frankenstein unbound: towards a legal definition of artificial intelligence. Futures. 1981;13(6):442–57.
15. Schank RC. What is AI, anyway? AI Mag. 1987;8(4):59.
16. Wang P. What do you mean by "AI"? AGI. 2008;171:362–73.
17. Dobrev D. A definition of artificial intelligence. arXiv preprint. 2012. arXiv:1210.1568.
18. Schuett J. A legal definition of AI. arXiv preprint. 2019. arXiv:1909.01095.
19. Krafft P, Young M, Katell M, Huang K, Bugingo G. Defining AI in policy versus practice. In: Proceedings of the AAAI/ACM conference on AI, ethics, and society. 2020. p. 72–8.
20. Wang P. On defining artificial intelligence. J Artif Gen Intell. 2019;10(2):1–37.
21. Cassez F, Dubreil J, Marchand H. Synthesis of opaque systems with static and dynamic masks. Formal Methods Syst Des. 2012;40(1):88–115.
22. Kissner L, Song D. Privacy-preserving set operations. In: Annual international cryptology conference. Springer; 2005. p. 241–57.
23. Lynn B, Prabhakaran M, Sahai A. Positive results and techniques for obfuscation. In: International conference on the theory and applications of cryptographic techniques. Springer; 2004. p. 20–39.
24. Mogul JC. Emergent (mis) behavior vs. complex software systems. ACM SIGOPS Oper Syst Rev. 2006;40(4):293–304.
25. O'Leary DE. Artificial intelligence and big data. IEEE Intell Syst. 2013;28(2):96–9.
26. Bartneck C, Lütge C, Wagner A, Welsh S. An introduction to ethics in robotics and AI. Cham: Springer; 2021.
27. Dornis TW. Artificial intelligence and innovation: the end of patent law as we know it. Yale J Law Technol. 2020;23:97.
28. Mezei P. "You ain't seen nothing yet"—arguments against the protectability of AI-generated outputs by copyright law. Arguments against the Protectability of AI-generated Outputs by Copyright Law. 2021. https://doi.org/10.2139/ssrn.3890051.
29. Ramezani SB, Sommers A, Manchukonda HK, Rahimi S, Amirlatifi A. Machine learning algorithms in quantum computing: a survey. In: 2020 international joint conference on neural networks (IJCNN). IEEE;2020. p. 1–8.