The Commonwealth

Commonwealth Cyber Journal \ 25
ISSN 2959-3018 (print), ISSN 2959-3026 (online)
thecommonwealth.org/cyber-journal

Special Section on Artificial Intelligence

Legal Application of Technical and Procedural Standards and Frameworks in the Combat Against GAI-Powered Cybercrime

Gilberto Martins de Almeida, Fernando Bourguy, João Farrel and Diego Semeraro[1]

Abstract

This article discusses the legal application of standards and frameworks as a possible approach for mitigating the increasing gap between the slow pace of legislative action and the fast evolution of cybercrime powered by generative artificial intelligence (GAI) systems. Its purpose is to demonstrate how standards and frameworks can fill in the blanks of existing cybercrime legislation, updating this with soft law if suitable. This has proved successful over time in various contexts.[2] This article analyses cybercrime legislation in Commonwealth countries,

1 Members of research institute Instituto Direito e Tecnologia (IDTEC) and of Martins de Almeida – Advogados law firm. Gilberto M. Almeida teaches computer and internet law at the Catholic University of Rio de Janeiro. Fernando Bourguy is a member of the Rio de Janeiro's Council for Data Protection. João Farrel is the secretary of the Committee on Data Protection of the Rio de Janeiro Bar Association. Diego Semeraro is a member of the Laboratory of Technology and Society Studies at the Federal University of Rio de Janeiro's Faculty of Law (LETS-FND).

2 Almeida, G. M. de (2011) *Legal Rules and Information Security Technical Standards: Possible approach for filling in the blanks of cybercrime legislation.* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1742962 (Accessed: 29 November 2023): 'Regarding specifically cybercrime legislation (and especially, the Budapest Convention, which is the one that has gathered accession from countries of all continents, so far), regulation by international conventions brings back the reflection on the possible convenience of combining hard law and soft law, and suggests it is worth investigating precedents, generally. In such connection, there are examples where international treaties have been enforced by means of reference to ISO standards. For instance, the oversight on compliance with the international convention on anti-doping has made use of a relevant ISO standard as criterion for judgment. There are, as well, examples of enforcement based on State-centered standards. For instance, the definition on disability and on mental illness provided by the World Health Organization norms and standards are issued under the institutional umbrella of the United Nations, which binds every State, and have supported enforcement both of international conventions and of national legislation. Therefore, independently of the nature of their origin, standards can be successfully used in conjunction with legal rules, as evidenced by practical experience, (...).'

with particular focus on Commonwealth small states.[3] It indicates that different countries have different national strategies, but that all Commonwealth countries take the same general approach.

Keywords: Generative artificial intelligence systems, GAI, Cybercrime, Criminal law, International law, Commonwealth law, Commonwealth small countries, technical standards, information technology.

Introduction

The use of artificial intelligence (AI) systems is widespread despite the lack of proper regulation in most Commonwealth countries. While AI in general can bring major economic and social benefits, generative artificial intelligence (GAI) is being used innovatively in cybercrime and is developing at a pace that is outstripping legislators.[4]

This article investigates whether regulation and interpretation of GAI-based cybercrime could be enhanced by standards or frameworks.[5] It defines AI and GAI and describes associated risks; considers the ecosystem of technical standards and frameworks relating to cybersecurity; analyzes statutory laws which need integration with other sources for construction and enforcement; identifies how legal rules may

3 In this article we use the definition of small country adopted by the Commonwealth: 'countries with a population of 1.5 million people or less; countries with a bigger population but which share many of the same characteristics. For example, Botswana, Jamaica, Lesotho, Namibia, and Papua New Guinea'. For this description and the list of Commonwealth small states see: The Commonwealth (n.d.) *Small States*. Available at: https://thecommonwealth.org/our-work/small-states (Accessed: 20 February 2024).

4 For an analysis of how technology could be faster than regulations and possible solutions see Fenwick, M., Kaal, W.A. and Vermeulen, E.P.M. (2017) *Regulation Tomorrow: What Happens When Technology is Faster than the Law?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834531 (Accessed: 22 February 2024) and World Economic Forum (2016) *Values and the Fourth Industrial Revolution: Connecting the Dots Between Value, Values, Profit and Purpose*. Available at: https://www.weforum.org/publications/values-and-the-fourth-industrial-revolution-connecting-the-dots-between-value-values-profit-and-purpose/ (Accessed: 22 February 2024)

5 Almeida, G. M. de (2016) Cybersecurity Policy and Lawmaking in the EU, US and Brazil, *Computer Law Review International*, 17(3), pp. 71–75. Available at: https://doi.org/10.9785/cri-2016-0303 (Accessed: 22 February 2024): 'In general terms, public and private cyber policy-makers are in a situation similar to those of cyberspace lawmakers. Resignation with relative safety has caused greater unpredictability, as increasingly obsolete, inconsistent controls have been targeted by cyber-criminals in their "venue shopping". Such circumstances should not be viewed as an inevitable context leading to inertia and to serious problem. There are ways for navigating among those difficulties, with appropriate balance and consistency. Indeed, meanwhile building "an international cybersecurity order has not been completed, sewing possible knots should be stimulated, with government and corporate stakeholders considering to adopt cautious, simple and proportionate" sets of interpretation and measures, based on widely accepted principles and on practical common denominators. Such mindset, moving from an impression that different national policies have turned unfeasible a global approach for managing cybersecurity to the perception that there are sound possibilities otherwise, may be the necessary first step in such direction.'

be complemented by standards and frameworks; and describes where and how this complementation could address GAI-powered cybercrime.

AI, GAI and associated risks

History and background

AI and GAI are not the first technologies to be made publicly available without regulation. Disruptive innovations are often developed before the general public is aware of them. They may become popular before parliaments can take normative action. This is because legislative due process depends on time-consuming discussion, negotiation and compromise, while technology developers move quickly dictated by market opportunities and expectations. This difference in pace has existed for a long time. But recent developments in, and use of, AI and GAI have intensified the contrast.[6]

AI and GAI have surpassed every statistic of rapid technological growth and acceptance.[7] The pace of this makes it difficult for civil society to learn about the risks posed by AI and how to protect itself against the many new kinds of AI-fuelled cyber-attacks.[8]

It appears that a new form of digital divide has arisen: the split between the massive number of AI users and the specialists concerned with its ethics and governance.[9] Regulators tend to stand between the two. They are sensitive to the need for technological innovation for the benefit of society, and are in favour of freedom of entrepreneurship. But also heed the warnings of law enforcement and cybersecurity advisers that certain principles and civil and criminal constraints will be imposed in order to inhibit AI-driven cybercrime.[10]

6 Fenwick, M., Kaal, W.A. and Vermeulen, E.P.M. (2017) *Regulation Tomorrow: What Happens When Technology is Faster than the Law?* Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2834531 (Accessed: 22 February 2024)

7 For instance, ChatGPT amassed 100 million active users within two months of its launch, making it the fastest-growing consumer application in history. See Hu, K. (2023) *ChatGPT Sets Record for Fastest-Growing User Base*. Reuters. [online] 2 Feb. Available at: https://www.reuters.com/technology/chatgpt-sets-record-fastest-growing-user-base-analyst-note-2023-02-01/. (Accessed on Nov. 29, 2023)

8 Notwithstanding the fact that cybercriminals have hacked networks and exploited social engineering on a virtually daily basis, drawing the attention of individuals, companies, governments and multilateral organizations – including the G7, which has promoted development and dissemination of a code of conduct for consideration by companies. See Habuka, H. (2023*) The Path to Trustworthy AI: G7 Outcomes and Implications for Global AI Governance*. Available at: https://www.csis.org/analysis/path-trustworthy-ai-g7-outcomes-and-implications-global-ai-governance. (Accessed on Nov. 29, 2023)

9 Specialists have adopted as source of reference, especially, UNESCO´s recommendations. See UNESCO (n.d.) *Ethics of Artificial Intelligence*. Available at: https://www.unesco.org/en/artificial-intelligence/recommendation-ethics#:~:text=Recommendation%20on%20the%20Ethics%20of%20Artificial%20Intelligence&text=The%20protection%20of%20human%20rights,human%20oversight%20of%20AI%20systems (Accessed: 22 February 2024).

10 In parallel, reported cases of criminal use of GAI are on the rise. In 2017, actor Gal Gadot was victim of deepfake abuse, when criminals edited her face on to a graphic scene. Since then, Chat-GPT and similar GAI systems have been made available for public use, at no charge, triggering escalation of similar cases. These now target not only celebrities, but anyone, with some preference for socially vulnerable groups exposed to all sorts of prejudice.

Assuming that AI can be used in different contexts and with various motives, it seems reasonable to predict that it may become the technology behind most common kinds of crime. This suggests the importance of studying whether, or how, that might affect the typology of criminal provision.

This issue is not exclusive to Commonwealth countries. Most developed nations have discussed it. However, there is a distinction based on the diversity of consequences for larger and smaller countries.[11] This distinction extends to the countries affiliated to the Commonwealth and has been acknowledged by the Secretariat.

Because cybercrime is a global issue, most developed and developing countries share some common ground and can combine knowledge and resources for devising anti-cybercrime strategies,[12] and concerted and more effective prevention and remedy.

Taking action against GAI-powered cybercrime within the Commonwealth requires consideration of both the symmetries and asymmetries of its countries and of the national circumstances and strategies relevant to cybercrime and AI.

Discussions about improving ways of tackling GAI-powered cybercrime should not be limited to a typology of criminal provisions. Technical definitions and procedures may be equally important.[13]

Combining legal rules and technical norms and frameworks must be considered carefully in order to prevent the risk of violating the principle of legality (*nullum crimen nulla poena sine lege*)[14] the prohibition of analogy *in malam partem*[15] and others.

11 'Finding response strategies and solutions to the threat of cybercrime is a major challenge, especially for developing countries. (...) The risks associated with weak protection measures could in fact affect developing countries more intensely, due to their less strict safeguards and protection.' See International Telecommunication Union (2009) *Understanding Cybercrime: A Guide for Developing States*, pp. 15–16. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Accessed: 22 February 2024).

12 'The development of technical measures to promote cybersecurity and proper cybercrime legislation is vital for both developed countries and developing countries. (...) Developing countries need to bring their anti-cybercrime strategies into line with international standards from the outset.' International Telecommunication Union (2009) *Understanding Cybercrime: A Guide for Developing States*, p. 16. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Accessed: 22 February 2024).

13 'A comprehensive Anti-Cybercrime Strategy generally contains technical protection measures, as well as legal instruments. (...) Cybercrime-related investigations very often have a strong technical component.' International Telecommunication Union (2009) *Understanding Cybercrime: A Guide for Developing States* pp. 15; 85) Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Accessed: 22 February 2024).

14 Gallant, K. S. (2008) *Legality in Criminal Law, Its Purposes, and Its Competitors*. Cambridge University Press. Available at: https://www.cambridge.org/core/books/abs/principle-of-legality-in-international-and-comparative-criminal-law/legality-in-criminal-law-its-purposes-and-its-competitors/E90DE2935156E2D2AD3EBD1E29C33A4B (Accessed: 22 February 2024).

15 'The authority applying criminal law should not interpret it extensively to the defendant's detriment, for instance, by analogy in malam partem.3 Accordingly, an offence must be clearly defined by law'. See Sanz-Caballero, S. (2017) The Principle of Nulla Poena Sine Lege Revisited: The Retrospective Application of Criminal Law in the Eyes of the European Court of Human Rights. *European Journal of International Law*, 28(3), pp. 787–817. Available at: https://doi.org/10.1093/ejil/chx049 (Accessed: 22 February 2024).

Understanding AI and GAI

This article has been written in response the Commonwealth Secretaria's call for papers focusing on GAI systems and cybercrime. Hence, in this article, AI mostly refers to GAI.[16]

GAI is a subset of AI systems that uses machine learning[17] algorithms to create new content such as images, videos, text and audio[18] on to which a user inputs a prompt. The system delivers a response to that prompt, 'interpreting', or rather trying to predict,[19] what the user wants. It then collects processes and/or repurposes pieces of information (building blocks) collected elsewhere, such as on the internet. By rearranging small pieces from different datasets, GAI systems can 'create' new sets in response to the prompt.[20]

Associated risks

Recent public availability of GAI has caused much discussion of the risks associated with its use. Understanding its varied panorama is key to identifying possible connections between technical and legal aspects. This, in turn, may justify combining legal rules and technical standards and frameworks. Knowing what crimes can be perpetrated using GAI is critical for this.

GAI-'authored' fake news is a serious risk, especially when associated with political elections, public health-related information, and unfair competition. Chat-GP's efficiency

16 AI itself could be defined as 'A machine-based system that is capable of influencing the environment by making recommendations, predictions or decisions for a given set of objectives, and by utilizing machine and/or human-based inputs/data to: a) perceive real and/or virtual environments; b) abstract such perceptions into models manually or automatically; c) use model interpretations to formulate options for outcomes'. OECD (2019) *Scoping the OECD AI principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO).* OECD Digital Economy Papers, No. 291, OECD Publishing: Paris. Available at: https://doi.org/10.1787/d62f618a-en (Accessed: 22 February 2024). For example, an autonomous vacuum cleaning robot could be thought of as an artificial intelligence, for 'sensing' and 'memorising' (a cleaning space, such as a house) by means of algorithms, to 'calculate' how best clean that space.

17 Machine learning (ML) can be understood as an AI system that can learn from data and generalise to unseen data, and thus perform tasks without explicit instructions (Kühl, N., Schemmer, M.,Goutier, M. & Satzger, G. (2022) Artificial intelligence and machine learning. *Electronic Markets*, 32. Available at: https://www.researchgate.net/publication/365294595_Artificial_intelligence_and_machine_learning .Accessed: 27 March 2024). It is able to develop new algorithms per se, by processing and interpreting similarities and differences in data, in order to cluster and profile them. Most GAI are powered by ML, and thus able to obtain positive or negative feedback from users on the quality of the delivered output, in comparison with the original prompt.

18 Routley, N. (2023) *What is generative AI? An AI explains*. World Economic Forum. Available at: https://www.weforum.org/agenda/2023/02/generative-ai-explain-algorithms-work/ (Accessed: 22 February 2024).

19 Agrawal, A., Gans, J. and Goldfarb, A. (2018) *Prediction machines: the simple economics of artificial intelligence*. Boston, Massachusetts: Harvard Business Review Press, p. 2.

20 Recently, Chat-GPT and certain other applications became famous as the first wave of publicly available GAI systems. Chat-GPT has been programmed to answer written prompts using common human language to such quality level that many answers could be mistaken by a human interaction. Dall-e is another example of GAI. Instead of answering in writing, Dall-e 'invents' new images upon a prompt. For audio, Beethoven.ai 'creates' new music.

in delivering trustworthy text may enable criminals to get fake news worded convincingly enough to inspire confidence. In addition, GAI can be applied together with search engine optimisation (SEO) methods to reinforce the virality of the message, increasing harmful effects for democracy, human safety and the free market.

Cybercriminals can also use visual or audio GAI systems. The ability to generate images or sounds may enable impersonation for spoofing, deep fakes, libel, defamation, ransomware and other criminal actions. Identity theft, to pave the way for asking money from a victim's close contacts, has become a common crime in many jurisdictions. With GAI to mimic voice, photos or videos, it is harder to see forged origin and malicious intent, increasing the likelihood of being caught by blackmailing schemes.

GAI may be used for crimes against the court system, by defrauding visual or audio evidence or simply by casting doubt on whether real evidence is indeed real. Discovery proceedings may be needed in order to assess whether certain evidence was produced by means of GAI, if litigating parties have not provided such disclosure.

With GAI, social engineering scams have spiked in recent times. Enhanced customisation ensures improved 'personalisation'. Documents are written with fewer errors reduce the barriers to non-sophisticated criminals. The ability to facilitate mass production of several but different versions of the same message can cheat anti-spam defences, improving the chance of a successful scam. A criminal may deepfake a manager´s voice to convince a subordinate employee to disclose confidential information by phone.

For hate crimes, child pornography and terrorism, GAI is known to have been used to generate racist or paedophilic images or terrorist propaganda. Despite efforts to prevent this, criminals and terrorists keep discovering ways to breach guardrails.

Intellectual property (IP) may be subject to criminal harm using GAI. For instance, the popularisation of non-fungible tokens (NFTs) has created a new market for their trade. Images embodied in an NFT may be forged ones, mimicking the style of a real artist. Moreover, a user may ask a GAI system to create a new trademark for their company, or a part of a new song or book, and the system could exploit existing IP on those, possibly infringing third-party rights when putting contents into the system or publishing similar results. There are ongoing lawsuits related to this.

Problems with GAI systems may originate from wrongful processing, which largely depends on the nature of the outputs. When putting data into a GAI system, there may be four kinds of outcome (as can happen with any data analytics system): known knowns, known unknowns, unknown unknowns and unknown knowns.

So-called known knowns are easy-to-solve problems that derive from the quality and reliability of the system itself. That is to say, the system and its operation have already been sufficiently tested so that the users know beforehand what problems might arise

from its use. Known unknowns, in turn, refer to a lack of trust by the user on the system when there are not enough data about its operation. For instance, when bad events are expected to be rare, it may be hard to know when and where known problems will arise.

Unknown unknowns are the most elusive. They refer to problems that have never arisen before. Because of that, users are not aware of their possibility. This can be addressed by training and by testing GAI in accordance with the so-called principle of precaution.

Finally, unknown knowns are problems that originate from excessive trust in a GAI system. This was observed, for instance, in the recent news of a lawyer using Chat-GPT to research favourable judicial precedents. 'Willing' to give a hoped-for response, Chat-GPT then fabricated a precedent by glueing together different real rulings.[21,22]

These problems may arise from common mistakes when handling data. For instance, mistakes such as undefined goals, error of definition, wrong capture of data, failed data measurement, poor data processing, bad coverage of collected data, improper data sampling, bad inference, and errors that are unknown simply because the representation of reality assimilated by the system has not grasped all aspects of that reality.[23]

Beyond those generic AI-related problems, GAI systems may also raise specific concerns, ranging from IP infringement to unauthorised processing of personal data, fostering criminal activities that rely on such illicit conduct to, directly or indirectly, perpetrate crimes.

In this connection, GAI systems have been used for cybercrime and for teaching people how to perpetrate it. The 'creative' nature of GAI has served the purpose of developing fake sounds, images, documents or videos, in ways that are hard to detect them *prima facie*, thus leading to fraud, identity theft and so-called social engineering.

21 'The new relationship that exists between knowledge, power, and duty at the dawn of the twenty-first century therefore requires a redefinition of the cautious attitude as well as new paradigms of responsibility and solidarity. As regards caution, we are currently witnessing the emergence in sociology and in law of a paradigm of security based on the principle of precaution, which was affirmed at the Rio Summit. This paradigm, born out of a fear of great disasters after the optimistic interlude of the years of faith in technology, rests precisely on the awareness of man's responsibility in this return of disaster.' (Bindé, J. (2003) 'Towards an Ethics of the Future', in Appadurai, A. *Globalization*, (ed.), Duke University Press, p. 100.

22 Maruf, R. (2023) *Lawyer apologizes for fake court citations from ChatGPT.* CNN Business. Available at: https://edition.cnn.com/2023/05/27/business/chat-gpt-avianca-mata-lawyers/index.html (Accessed: 22 February, 2024).

23 Yao, M., Jia, M., Zhou, A. and Zhang, N. (2018) *Applied Artificial Intelligence: A handbook for business leaders*. Middletown, De: Topbots, pp. 122–128.

In reaction to this, developers have adopted a methodology called 'alignment', by which an individual is responsible for continuously refining the system by feeding it again, with proper inputs, to avoid unlawful responses.[24,25]

The examples above show the difficulty of raising awareness about likely scenarios that could severely impair the rights of people and organisations. A repository of information on typical scenarios and their technical and legal implications is imperative given the unprecedented risks posed by GAI, which some describe as putting the future of humanity at risk.[26] This is where an ecosystem, formed of GAI-related legal rules, and technical standards and frameworks, may be a potential solution for providing reliable and proportionate guidance and enforcement.

Standards and frameworks

Standards are norms drafted and agreed on by experts[27] with the purpose[28] of setting uniform criteria, methods, processes or

24 However, it has been proved that users could circumvent it, by what is called 'shadow alignment'. That is, inserting opposite inputs, contaminating the system with unlawful content, and cheating it into thinking that the resulting answer is right. See Yang et al. (2023) *Shadow Alignment: The Ease of Subverting Safely-Aligned Language Models*. Available at https://arxiv.org/abs/2310.02949 (Accessed: 27 March, 2024).

An investigation by Brown University has found that certain barriers contained in Chat-GPT version 4 could not work if a less-well-known language is used, such as Scots Gaelic or Zulu ZDNET. Ray, T. (n.d.) *The safety of OpenAI's GPT-4 gets lost in translation*. Available at: https://www.zdnet.com/article/the-safety-of-openais-gpt-4-is-lost-in-translation/ (Accessed: 29 November 29 2023).

25 As a matter of fact, when Chat-GPT was publicly deployed, its failure to control usage for 'crime lessons' became viral. For instance, a user asked Chat-GPT where he could download pirated contents. Chat-GPT promptly responded that it could not give that kind of answer, as it related to criminal practice, but the user then inverted the question, asking which websites he should not visit to avoid downloading pirated content. The implemented controls were circumvented by the user by exploiting the naivety of the system, which ended up listing the websites that it had previously denied. Such an example demonstrates how easy it may be to use GAI for criminal purposes.

TechTudo. (2023) 4 provas de que o ChatGPT ainda não está preparado para os brasileiros. Available at: https://www.techtudo.com.br/listas/2023/05/4-provas-de-que-o-chatgpt-ainda-nao-esta-preparado-para-os-brasileiros-edsoftwares.ghtml (Accessed: 22 February 2024).

26 The Economist. (2023) *Yuval Noah Harari argues that AI has hacked the operating system of human civilisation*. Available at: https://www.economist.com/by-invitation/2023/04/28/yuval-noah-harari-argues-that-ai-has-hacked-the-operating-system-of-human-civilisation (Accessed: 22 February 2024).

27 The first experience of this is said to have been the creation of the International Electrotechnical Commission (IEC) in 1906.

28 Almeida, G.M. de (2016) Cybersecurity Policy and LawMaking in the EU, US and Brazil. *Computer Law Review International*, pp. 71–75. Available at: https://doi.org/10.9785/cri-2016-0303 (Accessed 22 February 2024): 'In the EU, standardization has been selected as a fundamental strategy against cyber-threats. The European Rolling Plan for ICT Standardization, and the IEEE Standards Activities in the Network and Information Security (NIS) Space, are examples of the attempt to build a platform of norms establishing patterns for encryption, removable storage, hard copy devices, and smart grids, so to better protect against malware and fix specific vulnerabilities. The European Network and Information Security Agency (ENISA) has alerted that the `Stuxne' attacks were a paradigm shift, which shall determine providing guidance on how to interpret the malware, its potential impact, and possible mitigation means, especially with regards to critical information infrastructures.'

practices.[29] These norms may be predominantly technical (specifications, test methods, units, terminology) or procedural (operating procedures, codes of practice).

The number of procedural standards, also known as standards on management systems and processes, has grown significantly.[30] Some of them are well known, such as the International Organization for Standardization (ISO) 9000 (quality) and ISO 14000 (environment).

Standards may be issued by so-called standards organisations or by individual groups or organisations. In the latter case, they are called de facto standards, being informally created and disseminated, like many technical frameworks referred to in this article. International standards organizations may be treaty-based or not. If they are, only governments can join as members and make them binding for all purposes and effects. If they are not, membership is also open to private parties, and standards are non-binding unless metrology national laws, also denominated altogether as normalisation system, make them mandatory (but limited to the domestic context).

Some organisations publish openly accessible standards, allowing them to be freely downloaded, copied and forwarded. Other organisations, such as ISO, charge for access to its standards to raise income.

ISO, for instance, is seen as reliable internationally. It is a non-governmental organisation (NGO), founded in 1946. Its prominence arises from its large membership, the volume of standards produced, and especially, the number of certifications issued worldwide based on its standards, or of projects inspired by them. Since its inception, ISO has addressed sectors as diverse as social responsibility, risk management, and information technology (the latter in conjunction with the International Electrotechnical Commission – IEC).

29 'Inter-state relations are no longer predominant in the international sphere, giving room to transnational relations. (...) Society of full rights. World of modulation, of constant formation required, of continuing control, of databases where cipher is the password as characterized by Deleuze, the new configuration overpass without eliminating the disciplinary society exhaustively described by Foucault according to the mold, the plant, the school, the test, the signature, the word of order. We are in the face of a society in network exercised by protocols and interfaces,' (Passeti, E. *Anarquismos e Sociedade de Controle* (Anarchisms and Control Society), quoted in Rodrigues, R. C. (2009) *O Estado Penal e a Sociedade de Controle* (The Criminal State and the Control Society), Revan, Rio de Janeiro, p. 37 (free translation from Portuguese).

30 '(...) it is now of interest to (...) create conditions for everyone to proceed on performing and deciding in the inside of government policies, in non-governmental organizations and in the construction of the electronic economy.' (Rodrigues, R. C. (2009) *O Estado Penal e a Sociedade de Controle* (The Criminal State and the Control Society), Revan, Rio de Janeiro, p. 37 (free translation from Portuguese). For the rapid pace of changing standards, see also Caprioli, E., Saadoun, Y. and Cantero, I. (2006) The Right to Digital Privacy: A European Survey. *Rutgers Journal of Law & Urban Policy*. Available at: https://rutgerspolicyjournal.org/wp-content/uploads/sites/26/2017/03/Caprioli_Saadoun_Cantero_European_Overview.pdf (Accessed: 22 February 2024).

The broad range of subjects addressed is the result of voluntary work performed by recognised standards authorities and experts from each country, distributed across several committees, subcommittees and working groups. Their systemic approach and uniformity of treatment are ensured by a single methodology for standards development (also including a 'fast-track'[31] procedure for documents with a certain degree of maturity at the start of a standardisation project, which could also be applied to rapidly changing technologies). This means that standards are agreed by consensus between government, industry, and other areas of civil society, with views and interests conveyed by each country's representative.

ISO claims copyright over its standards. These are available on payment for each copy. Additionally, ISO standards originate from the characteristics of its standards development process: open participation, consensual agreement, political neutrality, comprehensiveness, diversity, and – at least theoretically – no binding effect (unless international treaty-based). As a result, ISO standards are widely seen as credible, 'technical', up to date, international, commonly accepted norms, and worthy as guidelines for implementation or consultation.

In conclusion, standards may be a way of regulating matters at international and national levels,[32] to harmonise technicalities or procedures, to provide flexibility for individual countries to accept them or not, and to make them binding or not. This is central to philosophical, sociological and legal debates[33] about the convenience of a mix between hard law and soft law,[34] including whether or not soft law should be state-centred.

31 'Each standard goes through a six-stage process before being published as an ISO standard. The first stage is the proposal stage in which a need for a standard is determined and members are identified who are willing to work on it. The standards then enter the preparatory stage where a working draft of the standard is developed. When the working draft is completed, it enters the committee stage and is sent out for comments until a consensus is reached. The output of this stage is the Draft International Standard (DIS). The DIS then enters the enquiry stage where it is circulated among all member bodies and then voted upon. If a DIS does not receive 75% of the vote, it returns to lower stages and work on it continues. If it passes the enquiry stage, it becomes a Final Draft International Standard and enters the approval stage. During this stage it will again circulate through all member bodies for a final vote and again it must pass this stage with 75% of the vote. If the standard passes this stage, it enters the publication stage and is sent to the ISO Central Secretariat for publication.' See School of Computing and Information, University of Pittsburgh (n.d.) *II. A Brief History of ISO*. Available at: http://www.sis.pitt.edu/~mbsclass/standards/martincic/isohistr.htm (Accessed: 22 February 2024).

32 ISO standards are not necessarily endorsed by and incorporated into national statutory laws. Depending on each country's metrology normalisation system and preferences, ISO standards may not be accepted by local normalisation authorities or may remain aside from legal enforcement structures.

33 For example, Posner's comments on the functionality of the law, and Teubner's theory on autopoiesis. See Neves, A. C. 'O direito interrogado pelo tempo presente na perspectiva do futuro' (The law interrogated by present time under the prospective of the future), in Nunes, A. J. A. and Coutinho, J. N. de M. (2008) *O direito e o futuro – o futuro do direito* (The Law and the Future – the Future of the Law), Almedina: Coimbra.

34 On the combination of 'hard law' and 'soft law', see Peter Ulmer's and Peer Zumbansens's comments on the German Code of Corporate Governance (Ulmer, P. *Der Deutsche Corporate Governance Kodex – ein neues Regulierungsinstrument für Börsennotierte Aktiengesellschaften*, 166 ZHR 150 (2002), quoted in Zumbansen, P. (2009) *Law's Knowledge and Law's Effectiveness: Reflections from Legal Sociology and Legal Theory*. SSRN Electronic Journal. Available at https://doi.org/10.2139/ssrn.1415565 and https://digitalcommons.osgoode.yorku.ca/cgi/viewcontent.cgi?article=1126&context=clpe (Accessed: 22 February 2024).

Technical standards may have civil, administrative and criminal implications. On the one hand, they may be used as a source of interpretation for constructing, in the face of a given situation, the application of theoretical concepts such as duty of care, *bona fide* and others, directly associated with civil liability. On the other hand, they may fulfil requirements established in administrative rulings or decisions, by meeting principles of finality, morality, reasonableness and proportionality, as long as security practices recommended by standards match formal public policies and rules.

Furthermore, they may provide specific, updated content for the traditional typology of crimes such as forgery, falsification of documents (written, in audio or in video), theft, misappropriation and others, as they can be used to ascertain culpability based on wilful action, gross negligence, attempt, facilitation, mislead, damage and others. Relevant to this article, they may be valuable for law enforcement and adjudication for GAI-driven crimes.

International standards are often issued more quickly than the approval process for legislation in most countries. Updating technical definitions or procedures, which might be otherwise channelled through parliament, have been directed to standards organisations. Wherever GAI is involved, its rapid innovation seems more suitable for the attention of standards and frameworks than of legislative rituals.

Standards can apportion specific, up-to-date contents to regulations, especially for technological matters, characterised by fast evolution and obsolescence.[35]

In parallel to standards, frameworks have become increasingly widespread, especially in the areas of cybersecurity and AI,[36] where important contributions have been apportioned by entities such as the Organisation for Economic Co-operation and Development (OECD),[37] the National Institute of Standards and Technology (NIST)[38] and the Center for Internet Security (CIS).[39]

35 Specifically for AI, ISO has worked on applicable standards, an example of which is ISO/IEC JTC 1/SC 42, which structures ISO's standardisation programme on AI, covering terminology, data quality and other items. International Organization for Standardization (n.d.) ISO – ISO/IEC JTC 1/SC 42 – *Artificial intelligence*. Available at: https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0 (Accessed: 22 February 2024).

36 Frameworks have influenced UK and Canadian initiatives: the UK's Pro-Innovation AI Regulation White Paper, and Canada's draft Artificial Intelligence and Data Act.

37 Organisation for Economic Co-operation and Development (2022) *OECD Framework for the Classification of AI systems* Available at: https://www.oecd.org/publications/oecd-framework-for-the-classification-of-ai-systems-cb6d9eca-en.htmt (Accessed: 27 March 2024)

38 National Institute of Standards and Technology (2023) *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf (Accessed: 27 March 2024)

39 Center for Internet Security (2021) *Critical Security Controls Version 8*. Available at: https://learn.cisecurity.org/cis-controls-download. (Accessed: 27 March 2024)

In practice, frameworks are used to outline the full cycle of AI processes and management, while standards are often mostly concentrated on AI systems and procedures, although there is some overlap.

Blanket cybercrime laws

Criminal law is often regarded as *ultima ratio*[40] for punishing the violation of rights. Harsh criminal sanctions have fostered axiological social concerns, inspiring the principle of legality, pursuant to which only formal law, constitutionally enacted by lawmakers, can establish crimes and set relevant penalties.

However, the increasing complexity of social life, with technological expectations nurtured by contemporary living standards, requires leaving the door open to accommodate the inflow of scientific or technical advances and the repercussions on what legally constitutes a crime. This is where 'blanket criminal provisions' can play a significant role.[41]

Lawmakers are allowed to establish substantive contents of criminal provisions, and yet reserve accessory definitions for apportionment by other norms.[42]

For instance, blanket criminal law is often used to define thresholds on drug-related offences, as the definition of health and of addiction depends on scientific and technical knowledge.[43]

As mentioned above, this is also a way to quickly update a law, sort of 'futureproofing' the norm, without needing a new Bill to be brought before parliament. Inasmuch as scientific discoveries or new technical methods or terminologies cause different assumptions or goals, authorities are expected to refresh concepts.

A blanket provision may either quote the complementary norm, with a specific reference, or leave scope for modification by using generic terms (such as standards, code of practice or other).

40 'Criminal law provisions should be introduced when they are considered essential in order for the interests to be protected and, as a rule, be used only as a last resort'. In European Council (2010) The Stockholm Programme: An Open and Secure Europe. Serving and Protecting Citizens, OJ C 115, 4.5.2010. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010XG0504%2801%29 (Accessed: 22 February 2024).

41 '(...) blanket criminal provisions (...) are those which depend on complementation in order to comprehend the scope of its provision. That is, although the prohibited conduct is defined, its full enforcement depends, mandatorily, on complement from another source – statutes, decrees, regulations etc (...)'. See Greco, R. (2016) *Curso de Direito Penal: Parte Geral*, Rio de Janeiro: Impetus, p. 68.

42 Blanket criminal laws may be of homogenous or heterogeneous nature, as the complementary norm pertains to the same class of norms (that is, a formal law referring to another) or not (that is a formal law referring to an administrative regulation), respectively.

43 Legislation.gov.uk. (2016) *Psychoactive Substances Act 2016*. Available at: https://www.legislation.gov.uk/ukpga/2016/2/section/3 (Accessed: 22 February 2024).

An example of this is the Budapest Convention on Cybercrime, to which five Commonwealth countries (Australia, Canada, Cyprus, Malta and the United Kingdom) are parties and others (like South Africa) are signatories. Its text contains the following in many sections defining various cybercrimes: 'Each Party shall adopt such legislative **and other measures as may be necessary** to establish as criminal offences under its domestic law, (...)'.

Such wording calls for integration between legislative action and, presumably, standards and frameworks.

This is relevant to Commonwealth small countries which are also members of the Caribbean Community (CARICOM),[44] as the Commonwealth Model Law on Computer and Computer Related Crime is similar in content to the Budapest Convention.

Available information[45] shows that at least 23 Commonwealth countries have made use of the Budapest Convention or of the Commonwealth Model Law, 16 of which have legislation inspired by these, including Commonwealth small countries (Cyprus, Malta, Antigua and Barbuda, Barbados, Botswana, Brunei Darussalam, Jamaica, Maldives, Mauritius, Namibia, St Vincent and Grenadines, Samoa, Tonga, and Trinidad and Tobago). Therefore, the legal system of some Commonwealth small countries seems to admit the use of standards and frameworks to complement a criminal law.

Integrated application of legal rules, standards and frameworks for GAI-powered cybercrime

Different experiences of integration and combination[46] of legal rules and technical and/or procedural standards and frameworks have been originated through the activities of various players in international or national cybercrime regulation. Some countries stimulate the formation of an ecosystem by encouraging competitive national strategies

44 'In December 2008, ITU and the EU launched the project Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) to promote the ICT sector in the Caribbean region.' ITU. (n.d.) *Understanding cybercrime: Phenomena, challenges and legal response.* Available at: https://www.itu.int/en/publications/ITU-D/pages/publications.aspx?parent=D-STR-CYB_CRIME-2015&media=electronic (Accessed: 22 February 2024). One of the items of the project was the drafting of cybercrime legislation.

45 Global Project on Cybercrime (2013) *The Cybercrime Legislation of Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law Council of Europe contribution to the Commonwealth Working Group on Cybercrime.* Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3e4 (Accessed: 22 February 2024).

46 'Instead of reverting to "Command and Control" (CAC) type regulation, a new paradigm has emerged: non-state regulators have definitely pushed their way into regulation, even in traditional CAC areas like criminal law. They are increasingly integrated into decision making bodies, e.g. in financial services supervision.' International Scientific and Professional Advisory Council (ISPAC) of the United Nations Crime Prevention and Criminal Justice Programme (2006) Passas, N, and Vlassis, D. (eds) *The United Nations Convention against Corruption as a way of life*, p. 189.

(for instance, by legally recognising digital signatures, blockchains and AI), under the concept of so-called regulatory competition.[47]

Therefore, standards have become a crucial currency in international trade, both for governments and for the private sector (Lima, 2003).[48] Standards may influence and condition markets, and vice-versa, given their relevance for interpreting blanket laws.[49]

Contractual and extra-contractual situations arising from the use of GAI may cause multiple concerns to individuals and organisations, including questions such as who owns the data resulting from use of GAI, the level of confidentiality needed to protect data, protection against damaging outputs of the GAI system, and damages to consumers or even physical injury.[50]

Civil law relies on broad concepts such as *bona fide*, duty of care and others, to be responsive. However, those broad concepts may be applied subjectively by courts.[51] Therefore, they may be supported by standards, especially those focusing on procedural

47 The term 'regulatory competition' refers to a process whereby legal rules are selected (and de-selected) through competition between decentralised, rule-making entities (which could be nation states or other units such as regions or localities). Three justifications are usually given for regulatory competition: first, it allows the content of rules to be matched more effectively with the preferences or *wants* of the consumers of laws (citizens and others affected); second, it promotes diversity and experimentation in the search for effective legal solutions; and third, by providing mechanisms for preferences to be expressed and alternative solutions compared, it promotes the flow of information on effective law making. (Barnard, C. and Deakin, S. (2001) *Market Access and Regulatory Competition*. Available at: http://centers.law.nyu.edu/jeanmonnet/papers/01/012701-03.html (Accessed: 29 November 2023).

48 'The success of implementation of the standards of that organization is supposedly attributable to two factors: (I) for the increasing concern with global environmental problems; (II) for the increasing importance of "standardization" in international trade, in whatever sector. It is, no doubt, for such latter proposition that businesses of practically all countries in the world have adopted the patterns developed by ISO, as the non-adoption of referenced standards might cause much loss in view of the competition established in the current global economic scenario.' Bianchi, P. N. L. (2003) *Meio Ambiente: certificações ambientais e comércio internacional* (Environment: environmental certifications and international trade). Curitiba, Juruá, p. 100 (free translation from Portuguese).

49 Examples of legal and administrative norms were found in IAPP Research and Insights (n.d.) Global AI Legislation Tracker. Available at: https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf (Accessed: 22 February 2024).

50 For instance, we could imagine an employee of an underground train company searching on Chat-GPT for ways to quickly fix a problem in the carriages, and then Chat-GPT delivering a fake response without warning.

51 Almeida, G. M. de (2011) *Legal Rules and Information Security Technical Standards: Possible Approach for Filling in the Blanks of Cybercrime Legislation*. SSRN Electronic Journal. Available at https://doi.org/10.2139/ssrn.1742962. (Accessed: 22 February 2024): 'Whenever facing technical questions, Courts shall rely on experts or on rules of technical experience as sources for interpretation. Such rules shall be of common scientific or technical knowledge and are seen as a tertium generis between facts and legal rules, bridging them. Court decisions which make use of standards as source for interpretation are grounded on procedural law. They may also refer to standards not as sources but rather as subject of interpretation. This is particularly the case where standards are called upon to enforce statutory law which expressly invites taking them into account.'

content, such as those on governance (accountability, explainability, security and fairness).[52]

Such relevance is also acknowledged by courts, as most judges are not technological experts, and often depend on reports from experts to interpret complex cases.[53] Those reports translate technical facts into common language so that a judge can understand and consider these in their legal reasoning, bridging technical facts and legal rules.

Courts' decisions may also refer to standards, not as sources but rather as subjects of interpretation, notably when standards are called upon to enforce statutory law which expressly invites them to fill in the blanks.

Some statutory laws have acknowledged standards, in different ways, especially in the context of local normalisation structures. For instance, Europe´s General Data Protection Regulation (GDPR) refers to using standards for fulfilling data subjects' rights. Article 21(5) provides that 'in the context of the use of information society services', data subjects may exercise their rights to object 'by automated means using technical specifications'. Articles 20(1) and (2) describe how data subject to data portability shall be processed in a machine-readable format in order to be interoperable, where technically feasible. When reading 'technical specifications' and 'machine-readable format', it is possible to conclude that a market-driven norm commonly adopted could be used at scale to judge the lawfulness of the controller's response to these rights.

Also, some Commonwealth countries have already begun to regulate AI in different ways, including by using standards and frameworks.

52 Almeida, G. M. de (2011) *Legal Rules and Information Security Technical Standards: Possible Approach for Filling in the Blanks of Cybercrime Legislation*. SSRN Electronic Journal. Available at https://doi.org/10.2139/ssrn.1742962. (Accessed: 22 February 2024): 'In Criminal Law, there is often a thin frontier between intent and error, which is expected to draw the line separating guilty from non-guilty. Well-drafted, well-known standards may help determine the borders of such frontier. Criminal Law also differentiates between crimes of damage and crimes of danger. The number of types of crimes of danger has grown substantially in the latest decades – and many of them relate to the cyber environment. In such connection, standards may apportion interesting elements for interpretation on what materializes danger and on what constitutes reasonable care, which may be helpful for determining where intent (or gross negligence) was required and/or present, or not. (...) The subjectivity inherent to such broad concepts may be room for recourse to standards, especially the ones focusing on procedural contents, such as the ones on governance (especially, IT Governance, and Information Security).'

53 '(...) it is imperative to admit that, considering the state of the art in certain matter, time, and place, there is a knowledge accessible only to experts capable of dominating determined set of principles and of information, as there will always be a difference, regarding technical themes, between the general and approximated notion that the layman possesses and the deeper knowledge of the expert. Thus, any of us can approximately know the position that the planet Mars occupies today in the sky at certain time, but only an astronomer will be able to calculate its exact localization at the same time on February 23, 1950. The distinction, therefore, exists, and the way to draw it safely is by exclusion: it is an ordinary finding the one which is not of technical experience.' Fabrício, A. F. (2009) *Iniciativa judicial e prova documental procedente da Internet. Fatos notórios e máximas da experiência no direito probatório: a determinação do nexo causal e os limites do poder de instrução do juiz*, in *Livre-Arbítrio, Responsabilidade e Produto de Risco Inerente*, Renovar, Rio de Janeiro, p. 60 (free translation from Portuguese).

Canada has developed its Artificial Intelligence and Data Act (AIDA) to protect Canadians from high-risk systems and to ensure development of responsible AI. AIDA has adopted a risk-based regulatory approach, and envisages integrating the OECD AI principles, the NIST AI Risk Management Framework and the EU AI Act into Canada's regulatory system.

India has drafted a similar law, the Digital India Act,[54] to regulate high-risk AI systems. Indian authorities plan to develop an 'evolvable digital law', able to keep up to date with 'changing market trends, disruption in technologies, development in international jurisprudence and global standards for qualitative service/products delivery framework'. This meets India's National Strategy for Artificial Intelligence,[55] which recommends the use of technical standards for relevant matters, such as international standards as benchmark reference for lawmakers and safeguard criteria for AI developers. Hence, India has considered adopting technical standards to complement its statutory law.

Given the difficulty for general legislative bodies to enact statutory law on technology matters, some countries have opted for administrative regulatory approaches.

The Australian government has highlighted the application of technical standards in the context of the Australian AI framework and its 'AI Roadmap'.[56] Item 9.7 of the AI Roadmap provides that ISO, the American National Standards Institute (ANSI) and Standards Australia (AS) develop new standards for AI,[57] stressing that standards and system validation will be important trust-building assets for a future AI framework.

New Zealan's (NZ) government has issued an 'Algorithmic Charter', jointly developed by several institutions, including governmental and non-governmental organisations and a university,[58] thus adopting technical standards beyond statutory law. The charter recommends that government agencies use a risk matrix to assess the likelihood and impact of algorithmic applications. The NGO, NZ AI Forum, has published guiding principles designed to provide direction to AI stakeholders for developing a more comprehensive AI framework in the future.

A similar approach can be seen in the Australian, New Zealand and Jamaican legal frameworks for electronic identification (eID).

54 Ministry of Electronics and Information Technology of India (2023) *Proposed Digital India Act*, 2023. Available at: https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf (Accessed: 22 February 2024).

55 CSIRO (n.d.) *National Strategy for Artificial Intelligence*. Available at:

56 https://www.csiro.au/en/research/technology-space/ai/artificial-intelligence-roadmap%20. (Accessed: 22 February 2024).

57 Namely, system performance, safety, transparency, explainability, autonomy, privacy, interoperability, data security, data acquisition, data ownership, data quality, data formats and data storage. CSIRO (2019) *Artificial Intelligence Roadmap*. Available at: https://www.csiro.au/en/research/technology-space/ai/artificial-intelligence-roadmap%20 (Accessed: 22 February 2024).

58 New Zealand Government (2020) *Algorithm Charter for Aotearoa New Zealand*. Available at: https://data.govt.nz/assets/data-ethics/algorithm/Algorithm-Charter-2020_Final-English-1.pdf (Accessed 22 February 2024).

Finally, the United Kingdom (UK) is yet to enact the Artificial Intelligence (Regulation) Bill. Related matters such as data protection[59] and consumer protection[60] have already been regulated, and the UK may rely on such existing sectoral laws to establish AI limits. The UK government is also allying itself with NGOs, such as the British Standards Institution (BSI), in order to issue technical standards for the purpose of future regulation, as indicated in policy papers[61] and the UK's National AI Strategy.[62]

According to the IAPP's Global AI Legislation Tracker,[63] no Commonwealth small country has started to develop AI legislation, despite preliminary discussions.[64] However, some have enacted technical standards supporting legislation on privacy and similar rights, such as eID, that could overcome some of the challenges brought by GAI, such as unlawful use of personal information.

The Jamaican Data Protection Act of 2020 (JDPA)[65] provides obligations that depend on technical knowledge, *inter alia*, the need for the controller to adopt, and require from processors, appropriate technical security measures (Section 30(4)(a)). The JDPA also modulates the right to portability according to technical feasibility (Section 6(2)(C)(II)). Additionally, Jamaica enacted its National Identification and Registration Act, 2021 (NIRA) regulating the use of technical standards for storage, management, security and confidentiality[66] as stated also in its policy.[67]

Data protection legislation from Bahamas[68] and Barbados[69] does not explicitly mention reliance on technical standards. However, there is an obligation to adopt appropriate

59 GOV.UK (2018) *Data Protection Act*. Available at: https://www.gov.uk/data-protection (Accessed: 22 February 2024).

60 Legislation.gov.uk. (2011) *Consumer Protection Act 1987*. Available at: https://www.legislation.gov.uk/ukpga/1987/43/part/I. (Accessed: 22 February 2024).

61 GOV.UK. (2023) *A pro-innovation approach to AI regulation*. Available at: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper#fnref:68 (Accessed: 22 February 2024).

62 HM Government (2021) *National AI Strategy*. Available at: https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf (Accessed: 22 February 2024).

63 IAPP Research and Insights (2023) *Global AI Legislation Tracker*. Available at: https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf (Accessed: 22 February 2024).

64 UNESCO (n.d.) *UNESCO Caribbean Artificial Intelligence Initiative*. Available at: https://en.unesco.org/caribbean-artificial-intelligence-initiative (Accessed: 22 February 2024).

65 Jamaica (2020) *Data Protection* Act. Available at: https://japarliament.gov.jm/attachments/article/339/The%20Data%20Protection%20Act,%202020.pdf (Accessed: 20 February 2024).

66 Jamaica (2021) *The National Identification and Registration* Act. Available at: https://www.egovja.com/wp-content/uploads/2023/10/The-National-Identification-and-Registration-Act-2021.pdf (Accessed: 22 February 2024).

67 Jamaica (2016) *White Paper on National Identification System Policy*. Available at: https://opm.gov.jm/wp-content/uploads/2017/02/NIDS-Policy-October2016.pdf (Accessed: 22 February 2024).

68 Bahamas (2008) *Data Protection*. Available at: https://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/2003-0003.pdf?zoom_highlight=Police+act (Accessed: 22 February 2024).

69 The Barbados Parliament (2019) *Data Protection Bill*. Available at: https://www.barbadosparliament.com/bills/details/396 (Accessed: 22 February 2024).

security measures, which could imply awareness of technical standards issued or recognised by the relevant authority.

Similarly, in Trinidad and Tobago, it is possible to infer the connection with technical standards with its Data Protection Act calling for safeguards and standards that bind the commissioner.[70]

Certain Caribbean countries – including some Commonwealth small countries – are engaging in AI projects with the help of international entities, such as UNESCO[71] and the Caribbean Telecommunications Union (CTU)/International Telecommunications Union (ITU),[72] following in the footsteps of the HIPCAR project.[73] Considering Europe's and the USA´s drive to regulate AI, Caribbean countries need to follow the pace established by developed countries, in order to avoid the legal, technological and commercial gaps widening.[74]

Small countries need to devise their strategies, taking into account the fact that their environment may not be as resourceful as that of larger countries.

They may profit from using their existing cybercrime laws (and from observing international experience of cybercrime) as a starting point, and then using standards to fill in any blanks.

For instance, it is typical of cybercrime laws (including the Commonwealt's Model Law,[75] the Budapest Convention[76] and cybercrime law of small countries such as Barbados[77])

70 Parliament of the Republic of Trinidad and Tobago (2011) *Data Protection Act*. Available at: https://www.ttparliament.org/publication/the-data-protection-act-2011/ (Accessed: 20 February 2024)

71 UNESCO (n.d.) UNESCO Caribbean Artificial Intelligence Initiative. Available at: https://en.unesco.org/caribbean-artificial-intelligence-initiative (Accessed: 20 February 2024).

72 See https://ctu.int/event/ict-week/ (Accessed: 22 February 2024).

73 'HIPCAR was designed to support the Caribbean countries in improving their competitiveness by harmonizing approaches to ICT development. It brought together the Caribbean governments, regulators, service providers, civil society, private sector, regional and international organizations involved in ICT.' See ITU (n.d.) *HIPCAR Project*. Available at: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx (Accessed: 22 February 2024).

74 Skeete, K-A. D. (2022) *The Adoption of Artificial Intelligence within the Caribbean: Resuscitating the CARICOM's Single Market and Economy*. Cambridge University Press. Available at: https://www.cambridge.org/core/books/abs/international-perspectives-on-artificial-intelligence/adoption-of-artificial-intelligence-within-the-caribbean-resuscitating-the-caricoms-single-market-and-economy/BE948CF5D9623D001E9EF2161FA45F97 (Accessed: 22 February 2024).

75 '3. In this Act, unless the contrary intention appears: (...) "computer system" means a device or a group of inter-connected or related devices, including the internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function;'

76 'For the purposes of this Convention: (...) a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;'

77 '3.(1) In this Act (...) "computer system" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a programme, facilitates communication, performs automatic processing of data or any other function;'

to include a definition of 'computer system'.[78] This assumes that outputs will be generated 'pursuant to' determined programming, which is not strictly the case for GAI, the results of which may be unpredictable (that is, not 'pursuant to' relevant programming).

Therefore, small countries should rely on standards to make it clear that GAI falls within the definition of 'computer system', to the extent that AI systems relate to computer systems in spite of – possibly 'programmed' – black boxes.

For example, the diagnostics of a committee in charge of reviewing Jamaica´s cybercrime Act were: 'These general concerns include (...) the establishment of a Cybersecurity Authority and guidelines/standards for the protection of protected computers.'[79]

Families of standards can provide a comprehensive and integrated architecture,[80] that cannot be addressed by a single Act. For small states in particular, it would be difficult to address such architecture via a complex set of laws passed by parliament.

International standards virtually ensure worldwide recognition. Hence, it is both more practical and more beneficial for small countries to match their standards and legal rules governing GAI.

Standards may reinforce combatting GAI-powered cybercrime by providing several other helpful references (well beyond the definition of 'AI system', compared to 'computer system'). For instance, 'forgery' is a classic criminal typology, later extended to include spoofing, and now also 'deepfakes'. In short, standards can evolve, tracking new phenomena, without the need to introduce further legislation.

This is also relevant to GAI-fuelled cybercrime in the fields of IP, fraud and miscellaneous others.

Given the above, standards could help to regulate highly technical matters related to GAI in order to 'futureproof' legal gaps or to fill in the blanks.

78 This could be correlated with the expression 'data processing systems' present on the USA NIST definition of AI: '(1) A branch of computer science devoted to developing data processing systems that performs functions normally associated with human intelligence, such as reasoning, learning, and self-improvement.'

79 Linton, L. *New Offences Recommended for Inclusion in Cybercrimes*. Jamaica Information Service. Available at: https://jis.gov.jm/new-offences-recommended-for-inclusion-in-cybercrimes-act/ (Accessed: 22 February 2024).

80 For instance, among ISO standards, there are several norms pertaining to IA: ISO/IEC 23053:2022, which is specific to machine learning structures and systems; ISO/IEC 22989:2022, which addresses AI terminology and concepts; ISO/IEC 23894:2023, dealing with risk management in connection with AI; and ISO/IEC 42001, contemplating AI management systems.

Conclusion

This article indicates the urgent need[81] to combine legal rules with technical standards and frameworks to respond more effectively to the fast pace of cybercrime innovation, particularly GAI-powered cybercrime.

GAI has brought an unprecedented wave of cyber threats, with immense potential reach and economic and social relevance.

The complementation of legal rules with standards and frameworks may help Commonwealth small countries tailor cybercrime legislation,[82] by technically supporting legal provisions applicable to GAI-powered crime, in conformance with local background and scenarios.[83] At the same time, such an approach can ensure consistency with basic legal and technical patterns generally adopted by Commonwealth countries or derived from international context.

Such integration between legal rules and standards shall be constantly monitored and adjusted, given the fast pace of GAI's technological evolution.[84]

81 'In order to create a control mechanism over cyber space and some form of deterrent for cyber criminals, a number of countries around the world have reformed their existing laws and legislation; however, these have proven to provide vague and inefficient solutions. (...) Given the growth of cyber activities, the absence of a coordinated, comprehensive control framework has added to the spread of cybercrime in all shapes and forms. (...) A final recommendation has to do with the law itself in terms of content coverage and enforceability. (...) A number of countries have developed cyber laws which have many advantages(...). At the same time, however, they have various shortcomings, in terms of lack of coverage of certain crimes and/or the weight and severity of the penalty associated with the crime; (...)'. Karake, Z. and Al Qasimi, S.L. (2010) *Cyber law and cyber security in developing and emerging economies*. Cheltenham, UK; Northampton, Ma: Edward Elgar, pp. 1; 213; 231).

82 'Small and developing countries face difficulties in implementing the standards of the (Budapest) Convention. (...) One of the provisions that causes difficulties when it comes to implementation in small countries is the need to establish a 24/7 point of contact. (...) not all countries which have ratified the Convention have established such a contact point even countries which have provided such a contact point often only use it for limited purposes.' International Telecommunication Union (2009) *Understanding Cybercrime: A Guide for Developing States*, p. 127. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Accessed: 22 February 2024).

83 'Given the international nature of cybercrime, the harmonisation of national laws and techniques is vital in the fight against cybercrime. However, harmonisation must take into account regional demand and capacity. The importance of regional aspects in the implementation of anti-cybercrime strategies is underlined by the fact that many legal and technical standards were agreed among industrialised countries and do not include various aspects important for developing countries. Therefore, regional factors and differences need to be included within their implementation elsewhere.' International Telecommunication Union (2009) *Understanding Cybercrime: A Guide for Developing States* pp. 15; 85. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (Accessed: 22 February 2024).

84 On the need for a dynamic regulatory model, open to assimilating new developments and knowledge, see Murray, A. (2007) *The Regulation of Cyberspace: Control in the online environment*. Milton Park, Abingdon UK; New York, Ny: Routledge-Cavendish., p. 257: 'It is to be suggested that if we are to further our understanding of the regulatory environment within cyberspace (or any complex environment), we must, much like the quantum physicists of the early twentieth century, accept these limitations and use them to our advantage. For knowing what you do not know is as important as knowing what you do.'

About the authors

Gilberto Martins de Almeida teaches IT and internet law at the Pontifical Catholic University of Rio de Janeiro, and is a founder of the research institute IDTEC (Instituto Direito e Tecnologia), a partner at Martins de Almeida – Advogados, and a consultant to various divisions of the United Nations.

Fernando Felipe Bourguy de Medeiros is a partner at Martins de Almeida - Advogados, a member of the Rio de Janeiro Privacy Board, and an associate researcher at IDTEC (Instituto Direito e Tecnologia). He graduated in Law from the Federal University of Rio de Janeiro (UFRJ), and has concluded specialisation studies in law to become a magistrate.

João Farrel, deputy superintendent of the Data Privacy Committee of Rio de Janeiro's Chapter of the Brazilian Bar Association, is a researcher at IDTEC (Instituto Direito e Tecnologia), and an associate lawyer at Martins de Almeida – Advogados.

Diego Policani is a member of Technology and Society Studies Laboratory at the Federal University of Rio de Janeiro's faculty of law (LETS-FND), a researcher at IDTEC (Instituto Direito e Tecnologia), and a legal intern.