



## City Research Online

### City, University of London Institutional Repository

---

**Citation:** Chuah, J. (2022). Trust, Transparency and Technology—An Introduction to Smart Customs, Ports and Borders. *International Trade Law and Regulation*, 28(4), pp. 199-203.

This is the accepted version of the paper.

This version of the publication may differ from the final published version.

---

**Permanent repository link:** <https://openaccess.city.ac.uk/id/eprint/34119/>

**Link to published version:**

**Copyright:** City Research Online aims to make research outputs of City, University of London available to a wider audience. Copyright and Moral Rights remain with the author(s) and/or copyright holders. URLs from City Research Online may be freely distributed and linked to.

**Reuse:** Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge. Provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.

SPECIAL ISSUE: CUSTOMS MODERNISATION, TECHNOLOGY AND DIGITISATION

Issue Editors:

Prof. Jason Chuah, The City Law School, City, University of London, UK

Dr Trisha Rajput, University of Gothenburg, Sweden

## Trust, Transparency and Technology – An Introduction to Smart Customs, Ports and Borders

Jason Chuah

This Special Issue draws together works on the role and potentialities of smart technology and digitalisation for port, logistics and customs efficiencies. There is no denying that smart or automated ports and borders are seen not only as an important solution to resolving the problem of congestions or bottle-necks at ports and blockages in the logistics trail but also as a key plank in many a state's commitment to sustainable shipping<sup>1</sup>. Indeed, this theme is picked up by Karlsson who points out the often forgotten issues in the sector's drive to improving efficiencies. He argues that whilst customs systems such as the widely used Authorised Economic Operator (AEO) schemes, and indeed other trusted trader programmes have gone a long way at creating a level of trust between customs and supply chain participants, customs and other border agencies remain excluded from the substantial volumes of data generated by the private operators using modern digital tools. Without inclusion of customs and other border management entities in the data flow, border clearance inefficiencies will remain. Trade superhighways are being "constructed" to connect global value chains through major trade hubs. The research already shows that these superhighways are creating new levels of supply chain flexibility and visibility for manufacturers, suppliers, traders, and other supply chain participants and are generating the ability to create the 'just-in-time-always and 'just-in-case' supply chains of the future. However, much of this is put in jeopardy if border management authorities encounter difficulties processing the large amount of data being generated. It is a fact, as Karlsson reminds us, that border authorities (for example, customs, health agencies, fisheries authorities, security forces, police, immigration etc.) and governments have always had a fear of compromising national security by allowing its informational systems to be integrated into those of non-governmental, commercial operators. However, that conservatism needs to be challenged and the advent of new technology should certainly be embraced. Importantly, Karlsson observes that agencies, commercial enterprises and organisations at the border are inter-dependent on each other – where their data are not easily shared, that leads to a lack of trust which acutely affects those undertakings which have been pre-certified as being trusted (under an AEO scheme, for example). It thus reduces to an appreciable extent the usefulness of the AEO or trusted trader system. The scholarly point is perhaps to be drawn from Karlsson's work is that much of the current compliance and regulatory templates are based on a trust pessimism. But that absence of trust does not augur well for trade facilitation, especially as the global trading world is set to welcome the so-called Global Trade 2.0. The work is redolent of a point made with reference to the now discarded EU directive on supply chains that the AEO system has potential for recognition not only by customs but

---

\*\* Jason Chuah is Professor of Law at City, University of London. He and Dr Trisha Rajput, University of Gothenburg, are the Editors of this Special Issue.

<sup>1</sup> Chen, H. (2017) Applications of the cyber-physical system: a literature review. *Journal of Industrial Integration and Management* 2 (3): 1

other governmental bodies.<sup>2</sup> That potential has been underplayed and in creating Global Trade 2.0, integration between the AEO (and other trusted trader schemes) with data sharing systems is needful in two respects. First, the AEO system should be enlarged to other administrative organisations responsible for clearance at borders by being able to access the data flow, as appropriate. Secondly, the AEO system will need to ensure that a pre-condition for both the authorities (especially for the purposes of mutual recognition agreements with third countries) and the commercial operators that pre-agreed data should be shared using appropriate technological platforms. Countries should be encouraged to establish a fully digital single window system which permits a one-time only entry of data and one response only for imports, exports, and other trade related border processes. Those countries should ensure that standards harmonisation and development are properly provided and facilitated by law and regulation. That would ensure that compliant companies, those with AEO certification, could be identified and verified instantly without the need for extensive communications between the relevant parties. Much of this could be assisted by new digital tools and data analytics. To that end, I would submit that the role for artificial intelligence in the trade superhighway is going to continue to grow in relevance and significance.

This matter of artificial intelligence in the trade superhighway is one which is analysed and elaborated on by Basu Bal and Rajput. As a contrast and complement to Karlsson's work, Basu Bal and Rajput look at the matter of technological innovation, which they agree with Karlsson is needed for a joined up trade superhighway (or to use old fashioned parlance, logistical chain), from a public accountability angle. As customs increasingly use automated decision making (ADM) in their routine digital organising and management processes, it is highly likely that they will need to interact with artificial intelligence or AI driven systems. That will have, as Basu Bal and Rajput reason, to ensure that they are the right side of any present and emerging AI regulation. The matter is made all the more critical when in the use of data flow, third parties to whom data use functions have either been outsourced or onboarded. Customs, being the public authority, clearly is answerable for the safe and responsible of AI.

The contributors' paper presents a case study from Gothenburg Municipality to discuss ways in which customs and private IT suppliers need to ready themselves with a joint risk management programme to adhere to the upcoming European legislation on AI. The contributors at the University of Gothenburg draw on the legislation to argue that transparency as a requirement on the "provider" of AI services/systems raises particular challenges for customs authorities. Article 3(2) of the draft Regulation defines 'provider' as "a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge" whilst 'user' in art 3(4) means "'user' means any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the

---

<sup>2</sup> J. Chuah, "An Analysis of the proposed EU Legislation on Supply Chain Security" (2007) 4 Lloyds Maritime and Commercial Law Quarterly 523

course of a personal non-professional activity". In the main, it is where customs, as the public authority which has contracted to use an AI application developed by a commercial supplier

Despite the [anticipatory] legal requirement, I would add too that their focus on transparency is especially relevant too to Karlsson's emphasis on trust in his article. Trust is fostered both through cooperation in the managing and sharing the data and the transparency of the AI and other data processing mechanisms undertaken by the public authority in question. Basu Bal and Rajput draw on a case study involving the Gothenburg Municipality's use of ADM to place children in schools based on a set of pre-defined "objective" measures. However, the algorithm when working out geographic distances simply adopted "as the crow flies" distances without taking into account the fact that the city was divided by a river. The lack of transparency in how the system was deployed in the first place seriously damaged public trust in the local authority.

On a general point, other than data protection considerations, where the public authority uses AI to manage and apply the massive amount of data, such efforts might well fall within the scope of the newly proposed AI Act. Of special note too is the fact that AI is given a somewhat loose and broad definition. That breadth however is not entirely welcome. For example, Annex 1 of the proposed Regulation refers to "Statistical approaches, Bayesian estimation, search and optimization methods"<sup>3</sup>. This reference to statistical approaches is clearly expansive and potentially would cover almost all existing and future software that does not involve an element of machine learning<sup>4</sup> Statistical approaches could be fairly mathematical. For example, a software which computes the standard deviation of a set of data might well be deemed an AI system if this type of definition is adopted.<sup>5</sup> Perhaps a useful contrast might be had with the People's Republic of China's AI Development Plan (AIDP).<sup>6</sup> The PRC's AIDP though not a legislative instrument does flesh out what the PRC government considers to be AI for the purposes of legislative intervention. It tends to concentrate on what "basic theories" AI is founded rather than a purely systemic approach in

---

<sup>3</sup> Annex 1 describes AI techniques and approaches as: (a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning; (b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; (c) Statistical approaches, Bayesian estimation, search and optimization methods.

<sup>4</sup> See generally Ehsani S., Glauner, P., Plugmann, P. and Thieringer, F.M. (eds), "The Future Circle of Healthcare: AI, 3D Printing, Longevity, Ethics, and Uncertainty Mitigation" (Springer, 2022)

<sup>5</sup> See Chuah, Forward Planning – Regulation of Artificial Intelligence and Maritime Trade to be published in Zhao, L. and Jia, S. (eds) Maritime and Commercial Law in Europe and China (Routledge, 2022); available as City Law School, City, University of London Working Paper available at <https://openaccess.city.ac.uk/id/eprint/28256/> (accessed 1 July 2022)

<sup>6</sup> "新一代人工智能发展规划" State Council Document (2017) No. 35; there is no official translation of the strategy document at the time of writing. An unofficial translation might be found at <https://flia.org/wp-content/uploads/2017/07/A-New-Generation-of-Artificial-Intelligence-Development-Plan-1.pdf> For an exposition of the AIDP see Roberts, H., Cowls, J., Morley, J. et al. The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. AI & Soc Vol 36 59–77 (2021).

its attempt to define AI.<sup>7</sup> The AIDP considers that AI is premised on the following theories/notions:

*Big data intelligence theory*

*Cross-media sensing and computing theory*

*Hybrid and enhanced intelligence theory*

*Swarm intelligence theory*

*Autonomous coordination and control, and optimized decision-making theory*

*High-level machine learning theory*

*Brain-inspired intelligence computing theory*

*Quantum intelligent computing theory*

The PRC's approach seems narrower<sup>8</sup>, preferring to emphasise the presence of some machine learning methods or processes, or logic based procedures, than the EU's. Definitions are important when the emerging AI laws or regulatory plans are placing not only liability on the "users" and/or "providers" of AI services and systems but also like the EU Act, some are likely to have extra-territorial effect. Hence, it is pertinent that Basu Bal and Rajput look to examining whether and to what degree customs as a public authority might be subject to such AI laws. For customs to stay on the right side of the law and ethics, Basu Bal and Rajput stress that they need properly to understand the AI systems which are being used and undertake an inventory of all such uses or applications.

They point to customs' interaction with AI in discharging its public duties to prevent and prosecute criminals – a concern is that using AI for biometric and profiling purposes, often with prior consent, falls within the draft EU AI Act on responsibilities as regards "high risk" matters. A special concern, for me, too is the increasing use of sensor technology for various border control measures. These include visual-spatial, musical-rhythmic, verbal-linguistic, logical-mathematical and bodily-kinaesthetic sensing technology – all of which will mean that the AI systems are amassing Big Data and applying various algorithms to them. Governments certainly have a responsibility to keep their citizens safe and national security and public policy grounds have always been an important factor in all data protection (and in all probability, AI regulations). However, that does not mean that any high risk AI applications should not be properly accounted for and where there are lapses, liability should follow.

The role of smart technology at ports and borders is certainly the theme for this Special Issue. In Chagas Lessa's work, the focus is very much on how Brazil is embracing the notion of smart ports or more specifically "*Porto Sem Papel*" (paperless port). She focuses particularly on the structure of port ownership as a driver of smart port development in Brazil; the current legislation, it would appear, establishes *in the main* two types of project venture. First, where

---

<sup>7</sup> See Chuah, Forward Planning – Regulation of Artificial Intelligence and Maritime Trade to be published in Zhao, L. and Jia, S. (eds) *Maritime and Commercial Law in Europe and China* (Routledge, 2022); available as City Law School, City, University of London Working Paper available at <https://openaccess.city.ac.uk/id/eprint/28256/> (accessed 1 July 2022)

<sup>8</sup> It is arguable that the reference to theories leaves a large measure of discretion with the regulators.

the state or public authority takes both ownership of the port infrastructure and the operations of the smart port. Secondly, there is public ownership of the infrastructure but the private sector is responsible for developing the smart technology initiative. Given the role of the state in port management and operations, it is clear that legislative facilitation is needed if *porto sem papel* is to be successful. Chagas Lessa thus examines the enabling laws pointing out that the highly bureaucratic Constitutional provisions meant that any public private initiative will require various hurdles to be cleared but a positive development is the enactment of a law, RFB 143 of 11 February 2022. This act establishes the Application Programming Interface (API)<sup>9</sup>, a platform that centralizes the data, reducing the need to inform different institutions of same data and eliminating the need of paper reports. Like Karlsson indicated in his article, and supported by Chagas Lessa, such a system which operates on a shared interface means that Brazilian customs would be able to manage the data flow concerning movement of persons, cargo, and vehicles thereby better facilitating clearance and maximising security. That data flow, as is to be expected, shall rely in part on the capturing and processing of visual feeds, images and other sensory data. The use of AI, a matter of opportunity and concern, as raised by Basu Bal and Rajput, will thus be key. It might thus be suggested in the light of the optimism in Chagas Lessa's work, an appropriately framed AI regulatory response is also equally needful.

Chagas Lessa does raise an important issue which calls into sharp focus the need for better access to infrastructure finance for the development and establishment of smart ports. She discusses the positives and negatives of the different models of ownership and control over the smart port – Brazil had had, to some extent, to settle for a greater role for the state for socio-political and constitutional reasons. Other developing countries and emerging economies do have a choice depending on their constitutional constraints and access to infrastructure financing. It is thus suggested here that for Karlsson's vision of greater connectivity and the opening of the black box at the borders to become a reality, work is also very much needed in enhancing the provision and access to infrastructure financing in the global financial markets. In the jigsaw which this Special Issue had set out to discourse, the legal facilitation of infrastructure financing is another plank which must regrettably form the subject of analysis elsewhere.

## Conclusion

Smart ports or borders are very much in the spotlight in these days of severe logjams in the supply chains and logistic networks – whether caused by a sudden recovery phase from the global COVID-19 pandemic or geopolitical disruptions and friction. What the contributors have demonstrated here is the perennial challenge of balancing or reconciling the public and private interest. It is hoped that this Special Issue will demonstrate that this is not necessarily a zero sum game. There are key overlaps between the public and private interests. That mutuality of dependence cannot be underestimated in the move towards enhanced smart technology at borders and ports. The Gothenburg case study shows amply that the public-private demarcation is seldom clearcut. Such too is the premise in the new draft EU AI Act and the Brazilian customs law.

---

<sup>9</sup> See <https://api-docs.portalunico.siscomex.gov.br/swagger/rcnt.html> (accessed 1 July 2022)

Plainly, as the contributions to this Special Issue show, the orthodox presumption that relinquishing control of data (big or otherwise) by the state is *always* perilous needs to be challenged.







