

CONFERENCE PAPER

Balancing national legal protections of fisheries data and UNCLOS obligations in the age of AI

AuthorEva van Heukelom¹

Preamble

The following work was presented at the 12th ABLOS Conference, 7–8 October 2025, Doha, Qatar in the oral session *New technologies and maritime security*.

Abstract

Fisheries are an essential ocean industry, generating billions annually and supporting the livelihoods of millions worldwide. Effective management depends on governments' ability to collect and analyse fisheries data, including vessel movements, catch, and ownership information. This article examines the international legal frameworks that mandate such data collection, alongside national legal protections that may restrict data sharing beyond public authorities. It considers whether these limitations are justified, given the inherently transboundary nature of fisheries and the need for cross-border data exchange, particularly in efforts to combat illegal, unreported and unregulated (IUU) fishing.

Keywords

keyword fisheries · UNCLOS · fisheries transparency · fisheries data · AI · data protection · privacy

1 Introduction

Ask any fisheries inspector what matters most for effective management, and they will tell you: you cannot manage what you cannot see. In fisheries, "seeing" means having timely, reliable information on where, when, and how vessels are fishing, and what they are catching. This visibility underpins States' monitoring, control and surveillance (MCS) systems and is essential to meeting the obligation under the United Nations Convention on the Law of the Sea (UNCLOS) to conserve living marine resources on the basis of the best scientific evidence available and to maintain stocks at levels capable of producing maximum sustainable yield (UN, 1982, art. 61). Yet the legal framework that structures much of ocean governance was negotiated in a pre digital, paper based world, long before satellite tracking, real time databases, or artificial intelligence (AI) could be imagined as routine tools. At the same time, governments have

rapidly expanded domestic regimes for personal data protection, privacy, and commercial confidentiality, creating a complex landscape for sharing the very data that modern, AI enabled fisheries management depends on.

This article explores how national legal protections for fisheries related data, particularly personal data and commercially sensitive information, interact with States' obligations under the law of the sea to manage fisheries responsibly and cooperatively. It focuses on data generated by technologies such as the Automatic Identification System (AIS), Vessel Monitoring Systems (VMS), remote electronic monitoring (EM), satellite imagery, and electronic logbooks, which together provide a granular picture of human activity at sea. The aim is not to provide a doctrinal legal treatise, but to offer a clear understanding of the main legal tensions and to outline practical approaches for designing data systems and sharing

✉ Eva van Heukelom · eva@naturaljustice.nl

¹ Natural Justice, Noord-Brabant, Netherlands

arrangements that both respect domestic protections and support international obligations, including those embedded in UNCLOS and related instruments.

This article is based on the presentation of Eva van Heukelom at the ABLOS 12th Conference in Qatar. It was titled “Balancing National Legal Protections of Fisheries Data & UNCLOS Obligations in the Age of AI” and it is based on her PhD research at the Law of the Sea Department at the Universität Hamburg under supervision of Prof. Dr. Alexander Proelß.

2 Law of the sea in a pre digital world

UNCLOS was negotiated between 1973 and 1982 and is often described as the “constitution for the oceans” (UN, 1982). It distributes rights and duties between coastal States, flag States, and the international community across distinct maritime zones, including the territorial sea, exclusive economic zone (EEZ), and the high seas. Within the EEZ, coastal States have sovereign rights for exploring, exploiting, conserving, and managing living resources, coupled with duties to ensure that these resources are not over exploited and are conserved on the basis of the best scientific evidence available (UN, 1982, art. 61). UNCLOS itself, however, is striking for what it does not say: it contains no express references to ‘fisheries data’, ‘AIS’, ‘VMS’, or ‘artificial intelligence’. When it was being drafted, fisheries management was understood largely in terms of catch reporting, biological surveys, and paper based exchanges between administrations; satellites and digital databases were peripheral, and AI did not yet exist as a tool to support large-scale fisheries data analyses.

It would be misleading to assess UNCLOS’s fitness for modern fisheries governance by reading the 1982 text in isolation. Contemporary law of the sea is primarily captured in UNCLOS, together with a set of “implementation agreements”. To date, three implementation agreements have entered into force.. First, the 1994 Agreement relating to the implementation of Part XI of UNCLOS addresses deep seabed mining and is less directly connected to fisheries management (UN, 1994). Second, the 1995 Agreement for the Implementation of the Provisions of UNCLOS relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks (the Fish Stocks Agreement) significantly develops the obligations related to fisheries (UN, 1995). Third, the 2023 Agreement on the Conservation and Sustainable Use of Marine Biological Diversity of Areas Beyond National Jurisdiction (the BBNJ Agreement) seeks to fill governance gaps for biodiversity in areas beyond national jurisdiction.

The Fish Stocks Agreement is particularly important in the context of data. Its general principles explicitly recognize that “the timely collection, compilation and analysis of data are fundamental to the effective conservation and management of straddling fish stocks and highly migratory fish stocks” (UN, 1995, Annex I). It clarifies that data should be collected both from

fisheries on the high seas and in areas under national jurisdiction and compiled in a way that enables statistically meaningful analysis, including catch and fishing effort statistics as well as “vessel related and other data for standardizing fishing effort,” and information on non target and associated species (UN, 1995, art. 1). At the same time, the Agreement acknowledges that “confidentiality of non aggregated data shall be maintained” and specifies that dissemination is subject to the terms on which data have been provided (UN, 1995, Annex I).

Seen together, UNCLOS and the Fish Stocks Agreement articulate a clear expectation: States should collect, analyze, and possibly share fisheries related data in a timely and meaningful manner, including data closely tied to vessel operations, while respecting legitimate confidentiality concerns. The treaties leave the technical modalities, i.e. what technologies to use, how to structure databases, how to process data, largely to States and regional fisheries management organizations (RFMOs). This flexibility is what allows modern tools such as AIS, VMS, EM and AI based analytics to be integrated into MCS systems without revisiting UNCLOS itself. However, the same openness also means that much of the real friction arises from domestic law, not from UNCLOS: from data protection laws, constitutional privacy guarantees, intellectual property laws, administrative confidentiality rules, and transparency or freedom of information legislation.

Beyond the law of the sea, environmental law and international human rights law further reinforce obligations relevant to fisheries data. The growing recognition of the right to a clean and healthy environment, and the link between environmental degradation and the enjoyment of human rights, strengthens arguments that States must manage marine resources in a way that protects both ecosystems and the communities that depend on them. In this way, fisheries data sit at the intersection of multiple bodies of law: law of the sea, environmental protection, human rights, and domestic regulatory frameworks. International human rights instruments such as the International Covenant on Civil and Political Rights (ICCPR) also establish the right to privacy and private life (ICCPR, 1966, art. 17), which feeds into contemporary personal data protection regimes. Therefore, international human rights law provides protections to support the collection, storage, and sharing of fisheries data, but may also limit these due to conflicting interests. It is this interaction that will be explored in further detail in this article.

3 Technologies generating fisheries data

Over the last four decades, fisheries management has shifted from intermittent, low resolution observations to continuous, high resolution streams of digital data. AIS is a maritime tracking technology originally developed to enhance navigational safety and

collision avoidance by broadcasting vessel identity, position, course, and speed over VHF radio frequencies. Since around 2000, the International Maritime Organization (IMO) has progressively required AIS for vessels above certain tonnage thresholds engaged in international voyages, primarily through the International Convention for the Safety of Life at Sea (SOLAS) (IMO, 1974; Foley et al., 1990; see also relevant IMO instruments). AIS exchanges static data (such as vessel name, IMO number, dimensions, type), dynamic data (position, time stamp, speed over ground, heading), and certain voyage related information (such as destination and estimated time of arrival), although some of the latter are of limited relevance in fishing. From a fisheries perspective, AIS offers high frequency position and motion data that can be used to infer fishing behavior and gear type, but it has known limitations: some (smaller) fishing vessels are exempt; transponders can be switched off or manipulated; and AIS was never designed as an enforcement tool.

In contrast, VMS was developed specifically as a compliance and enforcement tool for fisheries (Paolo et al., 2024). VMS units, often satellite based, transmit vessel position, time, and sometimes speed or heading at regular intervals, typically providing multiple position reports per day with positional accuracy on the order of 100 meters. VMS carriage is usually mandated by fisheries legislation, license conditions, or RFMO measures for vessels above certain sizes or operating in particular fisheries. Unlike AIS, VMS data are generally not publicly accessible; they are transmitted to, and controlled by, fisheries monitoring centers (FMCs) or equivalent authorities, and commonly treated as confidential. For many States, VMS is the backbone of their MCS system and an indispensable source of information for meeting their UNCLOS Article 61 obligations.

Around these two core systems, a suite of complementary technologies has emerged. Remote electronic monitoring (EM) systems combine cameras, sensors, and onboard storage or transmission to document fishing operations, gear use, and catch handling. Satellite imagery, including both optical and synthetic aperture radar (SAR), can detect vessels regardless of whether transponders are active and can be cross referenced against AIS and VMS to identify dark or suspicious activity (Paolo et al., 2024). Electronic logbooks allow captains to submit catch and effort data digitally, improving timeliness and consistency. Together, these systems generate what can be described as fisheries “Key Data Elements” (KDEs): vessel location, date and time of activity; speed and course; vessel identity (including unique vessel identifier, name, and flag); fishing authorizations; gear type and fishing methods; catch quantity and composition; and related ownership and flag histories, including ultimate beneficial ownership.

These KDEs are not merely technical fields in a database. Several of them can overlap with protected

categories of information in domestic law. Vessel location, date, and time may constitute personal data where they can be linked to a specific individual, such as the vessel's master. Ownership and beneficial ownership data often include names, contact details, and nationality, which will in practice almost always qualify as personal data. Detailed fishing tracks and patterns may be argued to fall within trade secret protections, particularly where they reveal profitable fishing grounds. Understanding these overlaps is essential to designing lawful data sharing arrangements that still allow States and their partners to use modern tools, including AI or machine learning to better understand what happens at sea and to act on that information.

4 Personal data protection and privacy at sea

In recent decades, many States and regions have adopted comprehensive regimes for personal data protection, driven by concerns over surveillance, digitization, and the ease with which information can be aggregated and repurposed (Humble, 2021). The most influential of these is the European Union's General Data Protection Regulation (GDPR), which defines personal data as “any information relating to an identified or identifiable natural person,” explicitly including location data (EU, 2016, art. 4(1); see also Recital 71). The Council of Europe's Convention 108 extend similar principles to a broader group of States. Outside Europe, some jurisdictions have adopted dedicated data protection laws, such as Japan's Act on the Protection of Personal Information (APPI, 2003), while elsewhere protections derive mainly from constitutional rights to privacy or private life, as in the United States.

From a fisheries perspective, the central question is when, and to what extent, vessel tracking data constitutes personal data subject to these regimes. Individuals directly involved in fishing, i.e. masters and crew, could potentially be data subjects where data relates to them or can be used to identify them. Another group of individuals are legal or beneficial owners, whose names or identifiers may appear in licensing and registry data and whose economic interests are tied to vessel operations. Under instruments such as the GDPR, location data can be personal data when it is linked to an identifiable person, and this link may exist if, for example, public registers reveal the name of the master of a specific vessel and continuous VMS or AIS tracks show where that vessel is located at given times. The European Data Protection Supervisor has recognized that monitoring of vessel movements can involve processing personal data as long as the data can be linked to identified or identifiable individuals, including masters, owners, or crew (WP29, 2007).

At the international level, the right to privacy is enshrined in Article 17 of the ICCPR, which states that no one shall be subjected to arbitrary or unlawful

interference with privacy, family, home or correspondence, nor to unlawful attacks on honor and reputation (ICCPR, 1966, art. 17). Case law from human rights bodies and domestic courts has elaborated how this right applies in contexts such as communications surveillance, workplace monitoring, and GPS tracking of vehicles. However, I would argue the fisheries context is distinct. Vessels are generally workplaces rather than private homes, and monitoring via AIS or VMS is typically mandated by law as a condition of engaging in a regulated fishery. In addition, the open fields doctrine in the United States has limited the expectation of privacy in activities conducted in open areas, including at sea, although recent jurisprudence on persistent location tracking has highlighted potential privacy concerns (U.S. Supreme Court, 2012).

In practice, the connection between vessel tracking data and individual privacy is often narrower than stated. Comprehensive crew lists are generally not public, and in many cases only the name of the master or legal owner may be accessible in registers, such as those managed and published online by RFMOs. Nonetheless, in jurisdictions where location is explicitly included in the definition of personal data and where a link to an individual can be established, the publication or sharing of VMS or similar data may engage data protection rules, requiring a lawful basis, respect for purpose limitations, and appropriate safeguards. This creates uncertainty for administrations and for organizations seeking to promote greater vessel tracking transparency for the purposes of enhancing compliance and accountability at sea.

5 Commercially sensitive information and trade secrets

Separate from personal data protections, many jurisdictions recognize legal regimes protecting commercially sensitive information. Confidential business information may encompass any private details that a company keeps secret to maintain competitive advantage, including financial data, marketing strategies, unique processes, and, in the fisheries context, information about fishing grounds and patterns. Trade secrecy typically protects information that has commercial value because it is secret and has been subject to reasonable steps to keep it confidential. In some jurisdictions, fishing corporations have successfully argued that detailed information about fishing locations or techniques constitutes a trade secret and that mandating disclosure or sharing of this data would unlawfully undermine their competitive position.

Administrative law can reinforce these protections. Fisheries authorities often receive detailed data from companies under statutory or contractual obligations, and may treat this data as confidential, limiting dissemination even within government. In some cases, non disclosure agreements (NDAs) are used to reassure industry that data will not be shared beyond the collecting authority. Such NDAs may cover a broad

range of fisheries data, from VMS tracks to licensing details and ownership information. While these arrangements can secure industry cooperation, they may also undermine broader policy goals by preventing the use of data for cross agency collaboration, regional cooperation, or public transparency initiatives.

These commercial and administrative protections are sometimes invoked in ways that go beyond what is strictly necessary to protect legitimate business interests. For example, the assertion that any disclosure of fishing locations would destroy the value of fishing rights may be overstated in situations where data could be anonymized, delayed, or otherwise processed to mitigate competitive impacts while still supporting enforcement and research. At the same time, the global nature of fisheries, characterized by transboundary stocks and complex value chains, underscores that over protecting commercial information can facilitate opacity, including the use of flags of convenience, shell companies, and opaque ownership structures that enable IUU fishing and tax evasion.

6 Transparency laws and examples of proactive sharing

In contrast to regimes focused on confidentiality, some States have adopted transparency or access to information laws that facilitate proactive disclosure of government held data, including in the fisheries sector. Norway's Freedom of Information Act (Offentlegglova; JD, 2006) and Chile's Transparency Act (Ley de Transparencia; MINSEGPRES, 2008) are prominent examples. These laws require public bodies to facilitate access to information and establish transparency as a default, subject to specified exceptions for privacy, security, and commercial confidentiality.

In practice, Norway routinely publishes VMS based vessel tracking information for its fishing fleet, and Chile provides VMS data to organizations such as Global Fishing Watch, which combine it with AIS and other sources to produce public vessel tracking maps (Global Fishing Watch, n.d.). These practices coexist with robust personal data protection frameworks, such as the GDPR in Norway (EU, 1994, 2018) and constitutional privacy protections in Chile, demonstrating that legal systems can accommodate both privacy and public interest transparency when carefully balanced. They also show that once transparency is embedded in general administrative law, fisheries data can be treated as a form of public information rather than as purely confidential enforcement material.

These examples are not universally replicated. In the European Union, with the same GDPR protections as applicable to Norway, no Member State makes VMS data publicly accessible, often citing confidentiality or data protection concerns. Similarly, in jurisdictions such as Japan or the United States,

there is no consistent practice of publishing VMS data, although some aggregated or delayed information may be available. The result is a patchwork landscape where the same type of data, i.e. vessel tracks, authorizations, ownership details, is treated as confidential in some States, partially accessible in others, and public in a few instances.

7 UNCLOS obligations and emerging tensions

Against this domestic backdrop, it is important to recall that UNCLOS and related instruments impose international obligations that depend on the availability and, in many cases, the sharing of fishery related data. Article 61 of UNCLOS requires coastal States to ensure that living resources in the EEZ are not endangered by over exploitation and are managed based on the best scientific evidence available; Article 62 requires them to promote optimum utilization (UN, 1982). For straddling and highly migratory stocks, the Fish Stocks Agreement adds more specific data related responsibilities: States are to collect and share catch and effort data, as well as vessel related information, in a form that allows meaningful analysis and cooperative management, including through RFMOs (UN, 1995). The same Agreement recognizes the need to respect confidentiality of non aggregated data and to honor the terms under which data are supplied.

Meeting these international obligations requires States to design MCS systems that collect sufficiently detailed data and to participate in cooperative data exchanges, both domestically (across agencies) and internationally. For instance, restricting port access to vessels engaged in IUU fishing, one of the most effective tools currently available, depends heavily on access to vessel histories, authorization status, and activity patterns, which can be derived from VMS, AIS, and related sources. Similarly, the effective implementation of catch documentation and supply chain traceability schemes, which aim to ensure that buyers do not provide the economic incentive for IUU fishing, hinges on having reliable upstream activity data and being able to integrate it into verification processes. AI based analytics further increase the value of rich, long term data series, as they can reveal patterns of non compliance and guide enforcement resources to high risk vessels and areas.

Domestic legal protections can impede the flow of data needed for these functions. A coastal State may have VMS data capable of supporting advanced AI models to detect high risk behavior and to inform regional cooperation, but its data protection authorities or internal legal advisers may interpret personal data or trade secrecy rules as prohibiting sharing with neighboring States, RFMOs, or civil society partners, particularly in non aggregated form. Port States may wish to use risk profiles generated by third party platforms that combine multiple data sources, yet may find themselves constrained by national confidentiality

rules when it comes to contributing their own data to such platforms. Civil society organizations like Global Fishing Watch, SkyTruth, and Trygg Mat Tracking have demonstrated how combining AIS, satellite imagery, registries, and, where available, VMS can enhance transparency and support enforcement, but their access to official VMS data depends entirely on the willingness and legal capacity of States to share.

These tensions do not necessarily mean that UNCLOS is outdated or unfit for purpose. Rather, they reveal that the balance between different legal interests – privacy, commercial confidentiality, transparency, and environmental stewardship – is increasingly being struck at the national level, often without a clear understanding how this interacts with international fisheries obligations. While international law makes clear you cannot invoke national law to justify a failure to perform a treaty obligation (UN, 1969, art. 27), it is not always a given that sharing data beyond an FMC is required to fulfil UNCLOS obligations. Further, national laws frequently lack clear balancing tests for situations where, for example, trade secret protections intersect with environmental or human rights obligations, or where personal data protections must be weighed against the public interest in sustainable resource management. In others, the issue may be less legal than practical: limited administrative capacity, lack of familiarity with international law, or political concerns may inhibit data sharing even where legal avenues exist.

8 Navigating legal protections in practice

The challenge, then, is to navigate domestic legal protections in a way that respects individual rights and legitimate commercial interests while still enabling the data flows needed to fulfil UNCLOS obligations and to harness modern technologies for effective fisheries governance.

One approach is to minimize the extent to which fisheries data fall within the scope of personal data protection laws in the first place. This can be done by removing direct identifiers such as vessel names or unique vessel identifiers from data intended for broader dissemination, thereby attenuating the link between tracks and specific individuals aboard. Aggregating data over time or across fleets can further reduce identifiability, although aggregation may also diminish analytical value, particularly for detecting specific high risk vessels. Anonymization therefore appears to be a more promising strategy than aggregation where the goal is to retain useful granularity; even then, care is needed in small fleets or niche fisheries where re identification risks remain high.

Where personal data protection regimes clearly apply, e.g. States intend to share identified vessel tracks or to link them with public registers, organizations must ensure that data processing has a lawful basis and respects key principles such as purpose limitation and data minimization. Consent from data

subjects is one possible basis, but in the context of fisheries this may be logistically challenging and legally complex, especially where multiple crew members are involved and power imbalances exist. More promising may be legal bases grounded in the public interest or the exercise of official authority, particularly where domestic law or policy recognizes environmental protection, sustainable resource management, or transparency in natural resource exploitation as legitimate objectives. Some jurisdictions' data protection laws explicitly allow processing and sharing of personal data where necessary for tasks carried out in the public interest, though interpretations vary.

Commercial confidentiality and trade secret concerns can also be addressed through careful design of access regimes and contracts. Tiered access models can ensure that detailed, near real time data are available to core enforcement agencies, while more filtered or delayed data products are shared with regional partners, researchers, or the public. Data sharing agreements can specify permitted uses, protect against misuse by recipients, and recognize the need to safeguard competitive interests while still allowing analysis relevant to IUU fishing, environmental impacts, or supply chain integrity. Experience in jurisdictions such as Norway and Chile suggest that transparency and commercial interests need not be mutually exclusive, particularly when transparency is framed as a component of good governance and as part of the social license to operate.

Finally, technical experts and legal practitioners can work together to support legal and policy development. By clearly articulating what data are needed for particular management or enforcement objectives, what resolution and latency are required, and what safeguards can realistically be implemented, it becomes easier for lawmakers and regulators to craft rules that are both protective and enabling. This includes contributing to guidance within RFMOs, FAO led processes, or regional bodies on standardized, lawful sharing of fisheries data, and highlighting how improved transparency can reduce incentives for flags of convenience, opaque ownership structures, and other enablers of illicit activity at sea.

9 Is UNCLOS fit for purpose?

Returning to the core question whether UNCLOS is fit for purpose in modern times. At least in relation to fisheries and data, the analysis here supports a cautiously affirmative answer. UNCLOS, together with its implementing agreements, embeds a clear expectation that States will manage living marine resources based on sound, timely information, and will cooperate across jurisdictions to conserve and use these resources sustainably. While the Convention does not mention data or technology explicitly, it is sufficiently flexible to accommodate the transition from paper based reporting to satellite based tracking, from manual analyses to AI driven models. The law of the sea is not designed to prescribe the architecture of MCS systems or databases; instead, it sets objectives and allocates responsibilities, leaving the choice of tools and institutional arrangements to States.

Where the system falls short, it is often not because UNCLOS is inherently outdated, but because States have not fully implemented or coordinated the various legal regimes that affect fisheries data – international fisheries obligations, personal data protection, commercial confidentiality, transparency, and human rights. Excessive or unbalanced protections around fisheries data can inadvertently shield IUU fishing and undermine efforts to ensure food security and healthy marine ecosystems.

Conversely, thoughtful alignment of domestic laws with international obligations can enable greater fisheries transparency while still safeguarding individual rights and legitimate business interests.

The oceans are becoming increasingly observable, and AI is amplifying what can be inferred from vessel tracks, catch records, and environmental data. If managed responsibly, these advances can finally allow States to give practical effect to UNCLOS's call for conservation based on the best scientific evidence and for cooperative stewardship of shared marine resources. Achieving this will not require re-writing UNCLOS, but it will require careful work at the interface of law, technology, and policy: understanding the legal status of fisheries data, designing systems that respect both domestic protections and international duties, and maintaining an honest focus on the ultimate objective: healthy oceans and a thriving, lawful fisheries sector.

References

- APPI (2003). *Act on the Protection of Personal Information*. Japan.
- EU (1994). *Agreement on the European Economic Area* (OJ C 239/3, 1994; original adopted 1992, entered into force 1994. Council of the European Union. European Union, Brussels.
- EU (2016). *General Data Protection Regulation* (2016/679). *Official Journal of the European Union*, L119, 1–88. European Union, Brussels.
- EU (2018). Decision of the EEA Joint Committee No 154/2018 of 6 July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37 (containing the list provided for in Article 101) to the EEA Agreement [2018/1022]. *Official Journal of the European Union*, L183. <http://data.europa.eu/eli/dec/2018/1022/oj>
- Foley, J. D., van Dam, A., Feiner, S. K. and Hughes, J. F. (1990). *Computer Graphics – Principles and Practice* (2nd ed.). Addison Wesley.
- Humble, K. P. (2021). International law, surveillance and the protection of privacy. *The International Journal of Human Rights*, 25(1), 1–22.
- IMO (1974). *International Convention for the Safety of Life at Sea* (SOLAS). International Maritime Organization, London, United Kingdom.
- JD (2006). *Act relating to the right of access to documents held by public authorities and public undertakings* ('Offentleglova'). Justis- og beredskapsdepartementet (Ministry of Justice and Public Security), Oslo, Norway.
- MINSEGPRES (2008). *Ley No. 20.285 sobre Acceso a la Información Pública*. Diario Oficial de la República de Chile, Ministerio Secretaría General de la Presidencia, Santiago, Chile.
- Paolo, F. S., Kroodsma, D., Raynor, J., Hochberg, T., Davis, P., Cleary, J., Marsaglia, L., Orofino, S., Thomas, C. and Halpin, P. (2024). Satellite mapping reveals extensive industrial activity at sea. *Nature*, 625, 85–91. <https://doi.org/10.1038/s41586-023-06825-8>
- U.S. Supreme Court (2012). *United States v. Jones*, 565 U.S. 400.
- UN (1966). *International Covenant on Civil and Political Rights*. 999 U.N.T.S. 171. United Nations, New York, USA.
- UN (1969). *Vienna Convention on the Law of Treaties*. *United Nations Treaty Series*, 1155, 331.
- UN (1982). *United Nations Convention on the Law of the Sea* (adopted 10 December 1982, entered into force 16 November 1994). 1833 U.N.T.S. 397. United Nations, New York, USA. https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf (last accessed 30 March 2026).
- UN (1994). *Agreement Relating to the Implementation of Part XI of the United Nations Convention on the Law of the Sea*. United Nations, New York, USA.
- UN (1995). *Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks*. *United Nations Treaty Series*, 2167, 3. United Nations, New York, USA.
- WP29 (2007). *Opinion 4/2007 on the concept of personal data* (WP29). Article 29 Data Protection Working Party (WP29), European Union, Brussels.