

Legal 500

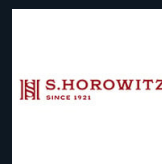
Country Comparative Guides 2026

Israel

Artificial Intelligence

Contributor

S. Horowitz & Co



Dr. Eyal Brook

Partner, Head of Artificial Intelligence Practice | eyal.brook@s-horowitz.com

Amit Steinman

Co-Managing Partner, Corporate and M&A Practice | amits@s-horowitz.com

Ran Vogel

Partner, Intellectual Property Practice | ranv@s-horowitz.com

Pini Azaria

Partner and a Co-Head of the Data Protection and Cyber Practice | pini.azaria@s-horowitz.com

Miriam Zaltsman

Partner, Corporate and Hi-Tech Practice | miriam.zaltsman@s-horowitz.com

Yaron Lestrel

Partner, Employment Practice | yon.llestrel@s-horowitz.com

Avner Itzhaki

Partner, Corporate and Commercial Transactions | avneri@s-horowitz.com

Israel: Artificial Intelligence

1. What is the legal definition of "artificial intelligence" in your jurisdiction, if any? If no definition exists, how do regulators or courts typically describe artificial intelligence?

There is no one definition of "artificial intelligence". On December 2023, Israel's Ministry of innovation, Science and Technology, in collaboration with the Ministry of Justice, published its first-ever policy on AI regulation and ethics (Israel's Policy on Artificial Intelligence – Regulations and Ethics – "The AI Policy"). According to the AI policy, "The field of artificial intelligence is a general name for the development of information technology, communication, and data science, enabling decision-making, making predictions, or performing actions by a computer at a high level of independence, in a way that simulates or is able to replace human intelligence".

The AI policy also states that among the many attempts to create a suitable definition, recently there is a trend of adopting the definition proposed by the OECD:

"AI System: An AI system is a machine -based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy".

It has been clarified, however, that this definition, is currently re-assessed due to current and expected development in artificial intelligence, and it may be updated in the near future.

The definition of AI in the financial sector is also based, inter alia, on the definitions adopted by the OECD and the European Union, with the necessary adjustments: "An AI system is a machine-based system that operates with varying levels of autonomy, and designed to generate output such as content, predictions, recommendations, or decisions, that may impact investors, customers, or the activity of the regulated firm".

2. Has your country developed a national strategy for artificial intelligence? If yes, what progress has been made in its implementation?

Are there plans for updates or revisions?

Israel has been termed "The Start-Up Nation". Israel's AI national AI program strategy capitalizes in Israel's entrepreneurial spirit, multidisciplinary collaboration, and innovative culture, aiming to leverage AI for societal and economic gains. With respect to the private sector, Israel's AI policy is premised upon the concept of "Responsible Innovation", based upon the need to support innovation, while fostering accountability and ethically-aligned design and uses of AI.

Such principles include:

- Sector-specific regulation – Empowering sectorial regulators to address AI risk and benefit within their domains.
- International interoperability of frameworks – fostering consistency with existing approached of leading countries and international organizations.
- A risk-based approach – AI regulation should be contextualized, weighing potential risks and benefits within specific use cases, compatible with the OECD trustworthy AI principles.
- Incremental Development & Regulatory Experimentation – using "soft" regulatory tools intended to allow for an incremental development of the regulatory framework.
- Multistakeholder Consultation – fostering multi-stakeholder cooperation between the public & the private sectors, academia and civil society organizations.

Public sector use of AI shall be promoted through dedicated funding, technological assistance to the relevant government units, and guidance in the fields of trustworthy AI and risk management.

See further:

<https://www.gov.il/BlobFolder/news/most-news20231218/he/Israel%20National%20AI%20Program%202024.pdf>
For further details regarding the recommendations on a regulation and ethics policy on AI, see:
https://www.gov.il/BlobFolder/policy/ai_2023/en/Israels%20AI%20Policy%202023.pdf

The National Artificial Intelligence Initiative (2025) aims to position Israel as a global leader in the field, with the

goal of enhancing quality of life, strengthening national resilience, and driving economic growth. To achieve this, the program focuses on establishing advanced computing and research infrastructures, expanding the high-tech talent pool, and developing local language processing capabilities. Additionally, it promotes the integration of AI within the public and private sectors while proactively preparing for its socio-economic impacts through responsible innovation. see: <https://innovationisrael.org.il/document/ai-national-program-2025/> The August 2025 report by the National Committee for Accelerating Artificial Intelligence led by Prof. Jacob Nagel, urged immediate action to position Israel among the world's top five AI nations by investing heavily in high-performance computing, advanced research, and high-level talent development. See: <https://www.gov.il/BlobFolder/news/event-ai050825/he/ai050825.pdf>

3. Has your jurisdiction adopted any AI-specific laws, regulations, voluntary standards, or ethical guidelines? If so, please provide a brief overview. If not, which existing laws could be/applied to artificial intelligence and the use of artificial intelligence, what are the main interpretive challenges, and are there any pending artificial intelligence legislative initiatives?

To date, no binding AI regulations have been formally enacted in Israel. However, on December 18, 2022, the Ministry of Justice released an influential legal opinion titled "Uses of Copyrighted Materials for Machine Learning," which examines whether machine learning (ML) developers can utilize copyrighted content for training Artificial Intelligence (AI) models without obtaining explicit authorization.

This pioneering opinion concludes that, with few exceptions, training ML models using copyrighted content is permitted under existing copyright frameworks. Specifically, it highlights that such training is primarily protected under the "fair use" doctrine, though some projects may also rely on the "incidental use" doctrine. Additionally, in scenarios where the copyrighted data is deleted immediately after the training phase concludes, the "transient use" doctrine may offer legal protection. Ultimately, the opinion's stance—that training AI systems generally complies with copyright law—aligns with prevailing international legal approaches, while explicitly noting that certain specialized ML applications remain excluded from this permissive scope. Several policy documents and recommendations for the responsible use of artificial intelligence have been

published, such as in educational institutions (<https://meyda.education.gov.il/files/Pop/0files/Annual-t heme/tashpad/Responsible-Use-policy.pdf>) and the public sector (<https://www.gov.il/BlobFolder/news/ai guide/he/%D7%9E%D7%93%D7%A8%D7%99%D7%9A%20%D7%9C%D7%A9%D7%99%D7%9E%D7%95%D7%A9%20%D7%90%D7%97%D7%A8%D7%90%D7%99%20%D7%91%D7%91%D7%99%D7%A0%D7%94%20%D7%9E%D7%9C%D7%90%D7%9B%D7%95%D7%AA%D7%99%D7%AA%20%D7%91%D7%9E%D7%92%D7%96%D7%A8%20%D7%94%D7%A6%D7%99%D7%91%D7%95%D7%A8%D7%99.pdf>) , alongside a comprehensive report on AI in the financial sector. Additionally, several bills have been proposed (for instance, regarding "deepfakes"), but they have not yet been enacted into law.

4. Are there legal requirements for artificial intelligence transparency, explainability, or audits? Are there obligations to disclose the use of artificial intelligence to customers/clients?

There is currently no Israeli law mandating disclosure for every use of artificial intelligence, but there is significant development of regulatory and ethical rules requiring it in several areas.

Industry-Specific Guidelines:

- Customer Service (General): The Supreme Court has ruled that when a consumer interacts with a chatbot or an automated service system, they must be provided with proper disclosure and transparency.
- Privacy Protection: The Privacy Protection Authority guidelines state that when collecting personal data from customers for AI processing, there is an obligation to inform them in advance that they are interacting with an automated system rather than a human, in order to enable informed consent.
- Legal Profession: The Ethics Committee of the Israel Bar Association published an opinion requiring transparency toward the client when AI is used to draft documents and pleadings, and also mandates human verification of all outputs.

5. Are there legal requirements or best practice expectations for human oversight and human-in-the-loop in artificial intelligence systems?

As of 2026, Israel does not have a formal, comprehensive law mandating human oversight or human-in-the-loop

frameworks for AI systems. The Principles for AI Policy, Regulation, and Ethics (2023) refers to the Recommendations on Accountability in Artificial Intelligence.

The principle of accountability establishes the need for a 'responsible entity' for artificial intelligence systems, which could be the developer or operator of the system. The principle emphasizes that artificial intelligence systems are created by humans, and therefore by default, humans are responsible for them, which reflects the importance of human involvement in artificial intelligence activities.

Key Supreme Court Precedent (March 2026): In a landmark ruling (Municipality of Ramat Gan), the Supreme Court established a clear legal requirement for human review, holding that relying blindly on AI outputs without human verification constitutes professional negligence or administrative flaw. It strictly prohibited delegating human discretion to automated systems when individual rights are impacted.

Regulatory Best Practices: The Privacy Protection Authority (PPA) guidelines strongly favor providing a human appeal mechanism for high-impact automated decisions. Additionally, the National Digital Directorate's Guide for Responsible AI Use in the Public Sector (May 2026) mandates active human intervention to mitigate risks, errors, and bias, setting HITL as the definitive national best practice standard.

6. Are there specific legal or regulatory requirements addressing algorithmic bias, discrimination, or fairness in AI systems (including gender bias)?

In Israel, there is currently no lateral, binding framework legislation or dedicated statutory law that specifically regulates AI, algorithmic bias, or discrimination (including gender bias). Instead, the country has opted for a sector-specific, "soft law" approach rooted in ethical principles and existing anti-discrimination frameworks.

The legal and regulatory landscape is characterized by the following:

1. Israel's Policy on AI Regulation and Ethics (2023)

In December 2023, the Ministry of Innovation, Science, and Technology, alongside the Ministry of Justice, released Israel's official AI Policy.

- **Key Principles:** The policy outlines core ethical

guidelines—closely aligned with the OECD AI Principles—which explicitly emphasize equality, the prevention of bias, and the avoidance of wrongful discrimination.

- **Sectoral Approach:** Rather than enacting a single blanket AI law (like the EU AI Act), the policy instructs individual sector-specific regulators (e.g., in banking, healthcare, or employment) to address algorithmic bias and fairness within their respective domains using risk-based, flexible, and "soft" regulatory tools (such as guidelines and voluntary standards).

2. Application of Existing Anti-Discrimination Laws

While there are no AI-specific statutes, developers and deployers of AI systems in Israel are fully subject to existing general laws. If an algorithmic system generates biased or discriminatory outcomes, it can be challenged under:

- **The Equal Opportunities in Employment Law (1988):** This prohibits employers from discriminating against candidates or employees based on gender, sexual orientation, age, race, religion, etc.
- **The Prohibition of Discrimination in Products, Services and Entry into Places of Entertainment and Public Places Law (2000):** This prevents automated pricing or service-provision algorithms from executing discriminatory bias based on protected classes.
- **Administrative Law:** Government and public bodies using decision-making algorithms are bound by Israeli constitutional principles of equality, fairness, and the prohibition of arbitrary discrimination.

3. Government and Legislative Discussions

State-level guidance encourages the implementation of auditing, validation of training datasets, and human-in-the-loop oversight to proactively mitigate these biases.

7. What legal frameworks apply to AI-related harm and defective artificial intelligence systems? Who can be held liable (developer, deployer, victim of the damage, others), how is liability allocated, and what burden of proof applies to victims?

In Israel, there is currently no dedicated, AI-specific statutory legislation addressing civil liability or defective

artificial intelligence systems. Instead, when AI-related harm occurs, courts and legal practitioners apply and adapt existing technology-neutral legal frameworks.

Currently, Israeli law does not feature a pre-established formula for the purpose of liability apportionment. In the absence of specific regulations, the liability of the developer, deployer, user, and victim is determined on a case-by-case basis under the general rules of applicable Israeli law. For instance, in claims grounded in tort law, liability is allocated according to the judicial doctrines developed under those frameworks. In this regard, if two or more parties are found liable for a tort, they are held jointly and severally liable for the harm. Although the internal apportionment among the tortfeasors does not directly affect the injured party's right to recovery, it is ultimately decided by the court. In making this decision, the court primarily assesses each tortfeasor's moral culpability and the causal link between their conduct and the resulting damage. For example, if both a developer and a deployer are found negligent and cause harm to an end-user, their liability will be partitioned based on their respective degrees of responsibility, taking these key factors into account.

Notably, while dedicated regulations on this matter have not yet been enacted, the Israeli government has outlined general guiding principles for future policy. These principles emphasize that those who create risks must assume responsibility for managing them, rather than shifting that burden onto other parties. Ultimately, liability will rest with whoever was responsible for the specific risk involved.

8. What cybersecurity obligations apply to AI systems?

As a general rule today, the various legal provisions dealing with information security and cyber protection apply to the security of AI systems.

Alongside sectoral legislation and regulation (such as the Law for the Regulation of Security in Public Bodies, 5758-1998; Circular 2016-9-14 on Cyber Risk Management in Institutional Bodies; Proper Banking Management Directive 364 on Information Technology Risk Management, Information Security, and Cyber Protection; the Israel Securities Authority directive to payment companies regarding technological measures and information security; and similar regulations) and various specific guidelines (such as the Privacy Protection Authority's Principles Document for Managing Information Security Risks in the Use of Open-Source Code), a central norm addressing the security of

information and the information systems in which it is processed is the Protection of Privacy Regulations (Data Security), 5777-2017, which addresses, among other things, the security obligations applicable to information systems that process personal data (the "Data Security Regulations"; see also, in this regard, the draft guideline of the Privacy Protection Authority: Applicability of the Privacy Protection Law Provisions to Artificial Intelligence Systems).

In practice, when applying the Data Security Regulations to artificial intelligence systems, this must be done while taking into account the unique characteristics of AI systems, which sometimes amplify existing risks and sometimes create new ones.

AI systems are often characterized, among other things, by long supply chains and more limited control over the use of data (including a limited ability to ensure deletion and prevent unauthorized uses). They are also characterized by the fact that their outputs change over time (whereas in conventional information systems the same input should always produce the same output, in AI systems the opposite is true—these are "learning" systems whose outputs typically change over time).

When AI systems are used to process personal data, the Data Security Regulations must be complied with (along with all other legal requirements regarding the processing of personal data in information systems). This includes ensuring that no prohibited uses of the data are made, that the use does not lead to exposure of data or allow various parties along the supply chain to use it for different, unagreed-upon purposes. Adequate control over the systems' outputs must be ensured, and there must be no exposure to uncontrolled uses or effects of the systems, such as deletion of data or the making of irreversible changes in connected systems.

It should be noted that while the Data Security Regulations do not apply to information systems that are not used for processing personal data, the conditions and principles set forth therein serve as useful guiding arrangements, with the necessary modifications, for systems not intended for the processing of personal data as well, in order to fulfill the general legal duty of care.

9. Is the use of artificial intelligence insured and/or insurable in your jurisdiction, including with cyber policies? Are there market trends, or limitations?

Only partially, mostly under and as part of extended cyber and professional liability coverage. In recent years, there

has been a noticeable trend toward approaching foreign insurers for more targeted policies that provide broader insurance coverage.

10. Can artificial intelligence be named as an inventor in a patent application filed in your jurisdiction? If not, what is the current legal position?

Similar to proceedings in other jurisdictions, Dr. Stephen Thaler attempted to register a patent application in Israel naming the artificial intelligence system DABUS as the inventor.

In March 2023, the Israeli Patent Commissioner issued a decision concerning whether an AI system may be recognized as an "inventor" under Israeli patent law. The Commissioner held that, under the current legal framework, an AI system cannot be named as an inventor. The Commissioner further held that recognizing AI as an inventor, or granting patents for inventions created without human involvement, raises policy questions that should be addressed by the legislature. Until such legislative change is made, only a human being may be named as an inventor in a patent application filed in Israel.

Dr. Thaler appealed the Commissioner's decision. On December 31, 2025, the Tel Aviv-Yafo District Court dismissed the appeal and affirmed the Commissioner's position that, under current Israeli law, an AI system cannot be named as an inventor. To the best of our knowledge, no appeal has been filed with the Israeli Supreme Court.

11. Do images or works generated by and/or with artificial intelligence benefit from copyright protection in your jurisdiction? If so, who is the authorship attributed to, and under what conditions?

The Israeli Copyright Act of 2007 requires that a work be "original" to benefit from copyright protection. Historically, both Israeli legislation and judicial doctrines presuppose that only a human being can be considered an "author". However, to date, no cases in Israel dealt with the issue of images generated by artificial intelligence, and the question of ownership in such works.

12. What are the main issues to consider when

using artificial intelligence systems in the workplace? Have any new regulations, or guidelines, been introduced regarding AI-driven hiring, performance assessment, or employee monitoring?

The main issues to consider when adopting artificial intelligence systems for candidate recruitment and employee management are concerns regarding bias, particularly where such bias may stem from the dataset used to train the system, which may also raise questions under privacy law, as well as concerns regarding hallucinations.

There is currently no specific legislation or regulation on this matter in Israel, although guidance may be drawn by analogy from recent Supreme Court case law concerning the use of artificial intelligence tools by public authorities, such as local authorities. Nevertheless, it is important to ensure that such systems comply with general Israeli labor laws, especially anti-discrimination laws and the case law of the labor courts, and that they provide reasoned outputs rather than making decisions as a "black box."

We recommend that our clients voluntarily adopt operating standards similar to legislation in places such as California or New York City in order to reduce exposure to claims, and to ensure that their agreements with AI tool providers or recruitment agencies include appropriate provisions regarding allocation of responsibility and indemnification arrangements.

13. What are the main privacy/data protection issues arising from artificial intelligence development and use (including training data)? Have data protection authorities issued guidelines or rulings on artificial intelligence, and what are the key takeaways?

As a general principle, training and using AI in conjunction with personal information raises challenges under most, if not all, principles of data privacy protection laws. Processing personal data with AI tools requires thorough examination of, and attention to, compliance with each principle.

While some data protection challenges also arise in other areas of law, each area has unique principles and rules that require independent examination. In Israel, the current approach is that AI's impact on each legal domain must be separately assessed and addressed.

For instance, training AI tools on datasets that include personal data requires full compliance with the law, both with respect to data collection and the intended use of that data.

The use of AI tools also carries information security risks and the potential for inadvertent disclosure of personal data, necessitating robust risk management strategies and preparedness for potential data breaches.

The logic of AI outputs is not always transparent. AI tools may introduce biases or lead to misuse of information. For example, AI tools used to make or support decisions may 'infer' facts not provided to them and rely on those facts in reaching decisions – even where the law prohibits reliance on such facts, whether generally or for the specific purpose for which the AI tool is being used. Such risks demand vigilance and proactive safeguards.

On April 28, 2025, the Privacy Protection Authority published for public comment a draft guideline regarding the applicability of the provisions of the Privacy Protection Law to artificial intelligence systems. The draft addresses the full range of aspects related to the development and use of artificial intelligence systems.

Following various responses and publications, we estimate that the draft will undergo updates and refinements before becoming a binding norm.

14. How is data scraping regulated in your jurisdiction from an IP, privacy and competition perspective? Are there recent precedents addressing the legality of data scraping for training of artificial intelligence systems?

Currently, Israeli law offers few guiding sources on the topic of data scraping for use in artificial intelligence systems in the areas of intellectual property, privacy, and competition law, and there is considerable uncertainty as to what is permitted and what is prohibited.

Regarding intellectual property and competition law, in one case adjudicated by a district court that dealt with the copying of data published (for a fee) on an online platform (accessible to all without charge) and its republication, after being rewritten, on another online platform accessible under different payment arrangements for employers and job seekers, the district court held that the copying of the data did not constitute copyright infringement and that, under the circumstances of that case, there was no unfair competition. The court gave significant weight to the fact that the copied information was not protected by copyright, and that even

if it were protected, the rights in it would belong to the publishers rather than to the client who originally posted it. The court also refused to enforce the terms of use that prohibited copying of the advertisements, on the grounds that those terms of use presuppose the existence of copyright in the advertisements when, in practice, no such copyright exists. The court further addressed the doctrine that developed in American law concerning copyright misuse. 1074-05 Ma'ariv v. All You Need (J. Michal Agmon Gonen)

An additional, non-binding source is an opinion published by the Ministry of Justice on the applicability of "fair use" to using protected works for AI training, which indicates that such use will generally constitute fair use, except in exceptional cases (such as training exclusively on the works of a single author) that require further examination. This does not mean that AI outputs will necessarily be non-infringing, but the use of protected works for training purposes, viewed through the lens of copyright law, is not in itself wrongful.

It is difficult to extract clear and sharp rules from these two sources, primarily because in the case adjudicated by the court, the copied information was not a protected work. It is possible that different wording of the terms of use, or the copying of protected works, would have led to a different outcome that would have affected the question of whether data may be scraped for the purpose of training artificial intelligence systems.

Regarding privacy protection, in a case adjudicated by a district court – 55466-07-21 Shmueli v. Margalit (J. Limor Bibi) – which dealt with the copying of advertisements from one real estate website to another, the court held that the mere use of personal information published to the general public does not violate privacy – either because it falls outside the scope of protected personal information, or because publication itself creates implied consent to re-use. Because the information in that case was used for similar purposes (advertising on a competitor's bulletin board), it is difficult to conclude that any other use would be permitted. Nonetheless, the ruling indicates that scraping itself is not prohibited; the primary focus is on the subsequent uses made of the scraped data.

Alongside this judgment, we note the draft guideline of the Privacy Protection Authority regarding the applicability of the provisions of the Privacy Protection Law to artificial intelligence systems. The draft presents a somewhat strict approach that requires both the consent of the data subject and the absence of any express or implied contradiction with the terms of use. We estimate that the final version of the policy will be somewhat more

definitive on this matter.

15. To what extent is the prohibition of data scraping in the terms of use of a website enforceable?

A prohibition on data scraping in a website's terms of use will not always be enforced, as the two cases above illustrate. In *All You Need*, the court expressed difficulty with a website owner's attempt to appropriate factual information posted by users – information that may not qualify as protected works and, even if it does, is likely owned by the users themselves.

Although in these two cases the court declined to enforce the prohibition, caution should be exercised in drawing broader conclusions. There will certainly be cases in which a contractual ban on data scraping is given effect, but each case must be assessed on its merits. Above all, terms of use must be tailored to the interests they seek to protect, so that the relevant provisions are not deemed unfair or invalid. The Uniform Contracts Law may provide guidance in this regard.

16. Does your country have a regulator or authority responsible for supervising the use and development of artificial intelligence? What are its powers and enforcement tools?

Israel's National AI Directorate was established within the Prime Minister's Office in September 2025 and is led by Director Brig.-Gen. (Res.) Erez Askal. Following its preliminary organization, the Israeli cabinet approved its formal national operating mandate and a sweeping multi-billion national AI program in May and June 2026 to position Israel as a global AI superpower.

The core objectives and strategic focus of AI development center on building sovereign infrastructure by driving supercomputing capabilities, heavily investing in advanced graphics processing units (GPUs), and establishing regional data center frameworks under the Server Farms Law, while concurrently laying the groundwork for a dedicated National Artificial Intelligence Institute through collaboration with local high-tech leaders and academia, expanding human capital and education by launching nationwide AI literacy programs in middle schools, broadening university degrees, and encouraging the repatriation of international experts, and placing a heavy emphasis on applied sectors to bolster national capabilities in Cyber AI, Physical AI, and defense against deepfakes.

17. How widespread is the adoption of artificial intelligence in businesses in your jurisdiction, and which sectors are leading?

The adoption of artificial intelligence in Israel is characterized by a stark, "two-speed" economy. While Israel remains a global powerhouse in terms of AI development and talent, the practical adoption of these technologies across its broader domestic business sector is highly concentrated.

The leading sectors are:

- High-Tech: Approximately 95% of employees in the high-tech industry use AI tools regularly, with 78% doing so on a daily basis.
- General Public: About 36% of the population in Israel use artificial intelligence applications.

Implementation in Businesses and the Public Sector

- General Businesses: Only about 28% to 30% of businesses in Israel actively utilize AI. The service sector leads with a 31% implementation rate, compared to commerce (16%) and manufacturing (20%).

18. How is artificial intelligence used in the legal sector, by lawyers and/or in-house counsels? Are AI-driven legal tools widely adopted, and what are the main regulatory concerns?

The artificial intelligence revolution has not bypassed law firms. Although the adoption of AI in the legal sector is still developing, AI tools are already being used in practice by many law firms as part of their daily work.

In Israel, most large and mid-sized law firms use various AI and LegalTech tools in areas such as contract review and drafting, legal research, legal operations, knowledge management, spend management, document review and eDiscovery, mergers and acquisitions, and regulatory compliance. Some firms also use internally developed AI-based tools to support specific work processes and improve efficiency.

The main regulatory concerns relate to information security, attorney-client privilege, privacy and cybersecurity. These concerns are particularly important where AI tools are used to process confidential client materials, sensitive commercial information, personal data or privileged legal advice. As a result, law firms are generally required to examine carefully the terms of use, data handling practices, security measures and

confidentiality protections of any AI tool before adopting it more broadly.

19. What are the 5 key challenges and the 5 key opportunities raised by artificial intelligence for lawyers in your jurisdiction?

5 Major Challenges of AI in the Legal Profession

- **Ethical and Legal Dilemmas:** Ensuring that AI tools operate strictly within established legal and ethical boundaries, while proactively tackling issues of algorithmic bias, system transparency, and liability.
- **System Integration:** Seamlessly incorporating artificial intelligence technologies into existing legal workflows and traditional frameworks.
- **The Skill Gap and Continuous Training:** Overcoming knowledge gaps by providing lawyers with comprehensive training, ensuring they can continuously adapt to rapidly evolving AI systems.
- **Regulatory Compliance:** Successfully navigating, understanding, and staying aligned with a constantly changing landscape of AI-specific regulations.
- **Impact on Employment and Professional Roles:** Managing how automation reshapes legal careers, while finding the right balance between technology adoption and preserving invaluable human expertise.

5 Major Opportunities of AI in the Legal Profession

- **Boosted Efficiency and Productivity:** Automating time-consuming, repetitive tasks such as document review, contract analysis, and preliminary legal research.
- **Higher Accuracy and Consistency:** Reducing human error to ensure a consistently high standard of legal output and administrative work.
- **Advanced Legal Insights:** Utilizing data-driven tools to uncover deeper insights, track trends, and conduct more comprehensive legal analyses.
- **Elevated Client Service and Experience:** Providing more tailored services through AI-driven applications, ultimately enhancing client engagement, communication, and overall

satisfaction.

- **Data-Driven Strategic Decision-Making:** Leveraging advanced data analytics to make more informed, strategic, and predictive legal decisions.

20. Where do you see the most significant legal developments in artificial intelligence in your jurisdiction in the next 12 months? Are there any ongoing initiatives that could reshape AI governance?

Looking ahead at the next 12 months, the most significant legal developments in artificial intelligence in Israel are expected to emerge through "soft," sector-specific regulation rather than formal, comprehensive AI legislation.

This trajectory is guided by Israel's Ministry of Innovation, Science, and Technology's inaugural policy on AI regulation and ethics (published in December 2023), which recommends concrete steps to foster responsible AI innovation in the private sector (the "AI Policy"). Like many initial policies published by national regulators and global organizations, the AI Policy sets high-level guidelines, goals, and recommendations regarding the regulation of AI development and use.

Consistent with Israel's established governmental approach, and considering the AI Policy's broad guidelines for sectoral regulators, Israel appears to have opted for a decentralized, sector-by-sector approach over a single, overarching AI law. This method focuses on a risk-based model grounded in the existing regulatory framework and globally accepted principles. The aim is to create a dynamic structure that harmonizes regulations across industries and activities while fostering innovation.

Given this approach, comprehensive AI legislation similar to the EU AI Act is not anticipated in Israel within the next 12 months, nor are dramatic legislative changes expected. Instead, specific policies and soft regulations are likely to be issued by various regulators, targeting particular sectors or topics. These targeted policies will likely address cases where the application of existing legal frameworks is insufficient, undesirable, or unclear, aiming to balance public interest issues with driving technological innovation.

Contributors

Dr. Eyal Brook

Partner, Head of Artificial
Intelligence Practice

eyal.brook@s-horowitz.com

**Amit Steinman**

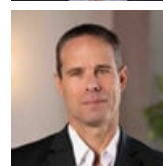
Co-Managing Partner, Corporate and
M&A Practice

amits@s-horowitz.com

**Ran Vogel**

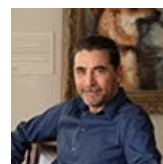
Partner, Intellectual Property
Practice

ranv@s-horowitz.com

**Pini Azaria**

Partner and a Co-Head of the Data
Protection and Cyber Practice

pini.azaria@s-horowitz.com

**Miriam Zaltsman**

Partner, Corporate and Hi-Tech
Practice

miriam.zaltsman@s-horowitz.com

**Yaron Lestrel**

Partner, Employment Practice

yaron.lestrel@s-horowitz.com

**Avner Itzhaki**

Partner, Corporate and Commercial
Transactions

avneri@s-horowitz.com

