151. [LegalZoom Launches Doc Assist in Beta, Combining the Power of GenAI and Our Independent Attorney Network](https://investors.legalzoom.com/news-releases/news-release-details/legalzoom-launches-doc-assist-beta-combining-power-genai-and-our)

Press Release

LegalZoom Launches Doc Assist in Beta, Combining the Power of GenAI and Our Independent Attorney Network

Sep 28, 2023

[PDF Version](https://investors.legalzoom.com/node/8316/pdf)

Demystifying legal documents for free, with the opportunity to talk with an attorney if you require legal advice

GLENDALE, Calif., Sept. 28, 2023 (GLOBE NEWSWIRE) -- [LegalZoom](https://www.globenewswire.com/Tracker?data=TT4iNB9e44-w94d5HIGclCjQVXOajJT0KBr9O9xLLKagyNiYntixWU9sRHop1zBnqm2Enpr_fC4EVw-Q1Yx8yg==), the No. 1 choice in online small business formations, today announced the beta launch of Doc Assist, a free document summarization product combining the power of generative AI and LegalZoom’s expertise in legal tech to help small businesses quickly review documents, stay organized, grasp core details swiftly and effectively, and gain access to expertise from vetted attorneys to make more informed decisions.

Doc Assist is a simple concept. Upload any legal document, and Doc Assist immediately provides the core details, distills crucial clauses, and prompts insightful questions tailored for that document type. Doc Assist combines cutting-edge Generative AI with our unique understanding of legal documents and their structures. Think of it as a tailor-made map for navigating the intricate world of legal paperwork.

Small businesses are afraid of attorneys. They think they’re expensive and use confusing and intimidating jargon. They don’t have a lot of time to find the right one, and when they do, they worry about spending too much time with them due to costs. This means many small businesses simply avoid attorneys and end up taking unnecessary risks – they sign leases, keep incomplete employee files, and often trust contracts from bigger, more established companies. The internet is awash in legal documents and many businesses adopt them as their own, without understanding what they are signing or sending for signature. 85% of current LegalZoom customers haven’t spoken to an attorney.  And it’s estimated that [40-60%](https://www.globenewswire.com/Tracker?data=2EAy_GcSCl3hLucJMcjNWXg5SPivO-wWrnZiYgQg6P4Pi05IBzfGiCclKTnyw5DmSTCjajeJU_QqqIG5EGFd_anDLCv0PkSQ4yIhH4qX89_D7U7D5hz1GX2xSKoaCPvG) of the population leaves its legal needs unmet.  The numbers get worse when considering underserved communities.  The problem is clear.

“Every small business should be able to understand the contracts it signs or sends for signature. Generative AI is an important component, but it’s best coupled with a credentialed attorney who is well versed in the type of legal document in question. LegalZoom is in a unique position to provide access to both,” said Dan Wernikoff, LegalZoom's CEO.

To try the beta version of Doc Assist and learn more about LegalZoom offerings, please visit [legalzoom.ai](https://www.globenewswire.com/Tracker?data=1DNUFCA9MzU7Bx498oLFMMhDs4v0Sqc_JdvKT-cxjB_ICcmc2j_QhaQToQ_K-i9hZcb8hDafZPasEqN7Wac8Qw==).

About LegalZoom.com, Inc.:  
LegalZoom is the leading online platform for business formation in the United States. Driven by a mission to unleash entrepreneurship, LegalZoom delivers comprehensive legal, tax and compliance products and expertise for small business owners through easy-to-use technology. From free business formations to business management solutions and professional advisory services, LegalZoom supports millions of small business owners and their families throughout the entrepreneurial journey. Founded on the belief that everyone should have affordable access to legal and financial expertise, LegalZoom empowers entrepreneurs to make their dream a reality. To learn more about LegalZoom, visit [www.legalzoom.com](https://www.globenewswire.com/Tracker?data=G62TJ2ZuSpofbiplYlvMGcmURLVIy9VE8FbgnjvOUPjkTXii5RnY5bufFqrCyQ-XAxLu1j-tzdSrJIx_6d0Kn0imYGJQLu4ESnNOnRaOrQc=).

Forward-Looking Statements:  
This press release contains forward-looking statements. LegalZoom intends such forward-looking statements to be covered by the safe harbor provisions for forward-looking statements contained in Section 27A of the Securities Act of 1933 and Section 21E of the Securities Exchange Act of 1934. All statements other than statements of historical facts contained in this press release may be forward-looking statements. In some cases, you can identify forward-looking statements by terms such as “may,” “will,” “should,” “expects,” “plans,” “anticipates,” “could,” “intends,” “targets,” “projects,” “contemplates,” “believes,” “estimates,” “forecasts,” “predicts,” “potential” or “continue” or the negative of these terms or other similar expressions. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond LegalZoom’s control. Actual results could differ materially from those stated or implied in forward-looking statements due to a number of factors, including but not limited to, risks detailed in “Risk Factors” section and elsewhere in LegalZoom’s Quarterly Report on Form 10-Q for the quarter ended June 30, 2023, filed with the SEC on August 8, 2023, as well as those in its subsequent filings with the SEC. These forward-looking statements are inherently uncertain and investors are cautioned not to unduly rely upon these statements. LegalZoom qualifies all of its forward-looking statements by these cautionary statements. Except as required by applicable law, LegalZoom does not plan to publicly update or revise any forward-looking statements contained in this press release, whether as a result of any new information, future events or otherwise.

152.  [AI principles](https://www.thomsonreuters.com/en/artificial-intelligence/ai-principles.html)

Data and AI ethics principles

Thomson Reuters will adopt the following Data and AI Ethics Principles to promote trustworthiness in our continuous design, development, and deployment of artificial intelligence (“AI”) and our use of data:

That Thomson Reuters use of data and AI are informed by our [Trust Principles](https://www.thomsonreuters.com/en/about-us/trust-principles.html).

That Thomson Reuters will strive to partner with individuals and organizations who share similar ethical approaches to our own regarding the use of data, content, and AI.

That Thomson Reuters will prioritize security and privacy in our use of data and throughout the design, development and deployment of our data and AI products and services.

That Thomson Reuters will strive to maintain meaningful human involvement, and design, develop and deploy AI products and services and use data in a manner that treats people fairly.

That Thomson Reuters aims to use data and to design, develop and deploy AI products and services that are reliable, consistent and empower socially responsible decisions.

That Thomson Reuters will implement and maintain appropriate accountability measures for our use of data and our AI products and services.

That Thomson Reuters will implement practices intended to make the use of data and AI in our products and services understandable.

Thomson Reuters will use employee data to ensure a safe and inclusive work environment and to ensure employee compliance with regulations and company policies.

We believe these Data and AI Ethics Principles will provide our colleagues and partners with the right foundations to build trustworthy, practical, and beneficial AI for our customers. These Data and AI Ethics Principles will evolve as the related industries continue to mature.

153.  [Comprehensive impact of AI](https://zegal.com/blog/post/the-comprehensive-impact-of-ai/)

The Impact of Artificial Intelligence on Legal Practices

The intersection of technology and law brings forth a myriad of opportunities and challenges that demand our attention. From simplifying labor-intensive tasks to revolutionizing legal research methodologies, AI is fundamentally altering the way legal professionals operate. As we start using it more widely, it becomes imperative to dissect the various facets of its impact, ranging from enhanced efficiency in document analysis to the ethical considerations surrounding autonomous decision-making algorithms. Here we will discuss the profound implications of this innovation on legal proceedings.

We aim to explore the potential advantages and ethical dilemmas emerging as machines become a huge part of jurisprudence. Through an analysis of real-world implementations and foreseeable obstacles, our goal is to provide readers with a thorough comprehension of how AI is fundamentally transforming legal practices.

Legal Research and Document Review

Legal research and document review have long been integral aspects of legal practice, demanding considerable time and resources. AI technologies, such as machine learning and natural language processing, are changing how specialists conduct analysis and examine vast amounts of documents. Let’s take a look at some of the advantages this development brought to these procedures.

Efficiency and Speed. It can analyze and sift through massive volumes of legal data in a fraction of the time it would take a human researcher. This acceleration enables workers to access relevant information swiftly, allowing them to focus on higher-value tasks.

Accuracy and Precision. Natural language processing algorithms possess the capability to comprehend context, extract pivotal concepts, and identify precedents with a remarkable level of precision. This not only diminishes the probability of errors but also elevates the quality of legal analysis.

Predictive Analytics. By examining historical case outcomes and legal precedents, AI can assist lawyers in making data-driven predictions about the potential success or challenges of a case.

Cost-Effective Solutions. Automating routine research tasks allows specialists to allocate their time more efficiently, reducing the overall hours spent on research. This, in turn, can result in increased productivity and cost-effectiveness.

Due Diligence in Transactions. These tools can analyze contracts, identify key clauses, and highlight potential risks or compliance issues. This not only expedites the due diligence process but also ensures a more thorough and comprehensive review.

Contract Review and Management

Dealing with any contracts requires meticulous attention to detail and a comprehensive understanding of legal language. AI technologies have become powerful instruments for automating and improving the process. These algorithms allow us to comprehend and analyze contracts, extracting key information and identifying critical clauses faster. This acceleration gives an opportunity to expedite the review process, enabling workers to handle larger volumes of contracts.

Those innovations bring a level of precision to contract assessment that is challenging to achieve through manual processes alone. They can identify inconsistencies, flag possible threats, and confirm that agreements comply with legal standards.

Moreover, AI facilitates the automation of abstraction and summarization. Legal practitioners can use these tools to extract fundamental data points and generate concise summaries of complex contracts. This feature is particularly valuable in scenarios where a quick overview of terms and obligations is needed.

Also, it contributes to the entire contract lifecycle management process by automating routine tasks associated with creation, negotiation, and renewal. [Automated workflows](https://www.jotform.com/blog/workflow-automation-examples/) and reminders help ensure that critical dates and obligations are not overlooked.

Predictive Analytics for Case Outcomes

Predictive analytics empowers specialists to make data-driven decisions by analyzing patterns and trends in historical data. By considering factors such as case type, jurisdiction, judge, and relevant precedents, lawyers can gain insights into the possible outcomes of a case. This approach improves decision-making, allowing legal practitioners to develop more informed and strategic tactics. What are some other benefits?

Risk Assessment and Mitigation. By identifying patterns associated with successful or unsuccessful outcomes in similar cases, lawyers can gauge the potential risks and challenges a case may present. This allows for proactive risk mitigation strategies and better-informed client counseling regarding the probable results of legal proceedings.

Resource Optimization. By focusing efforts on cases with a higher likelihood of success or by identifying pivotal factors influencing case outcomes, lawyers can optimize their time, energy, and resources. This leads to boosted efficiency in managing caseloads and enhances overall productivity.

Case Preparation. Understanding the likely trajectory of a case allows experts to tailor their strategies, arguments, and evidence presentation accordingly. This strategic approach improves the general preparedness of legal teams and raises the likelihood of achieving favorable results.

Client Counseling. Lawyers can use data-driven insights to communicate potential results realistically, helping clients understand the risks and uncertainties associated with their legal matters. This transparency fosters trust between specialists and their clients.

Automation of Routine Tasks

The legal industry is traditionally characterized by meticulous and time-consuming tasks. The incorporation of Artificial Intelligence is transforming this niche through the automation of routine processes. Mundane and repetitive tasks, such as document drafting, data entry, and administrative processes, can be automated, freeing up valuable time for workers to concentrate on more complex and strategic aspects of their jobs.

These tools enable the creation of document templates and the automatic generation of documents. This includes contracts, agreements, and other routine paperwork. You can input key variables, and the automation system generates customized records, reducing the time spent on manual drafting.

“alt”=”task automation”

Also, it facilitates data entry processes by extracting, categorizing, and organizing information from various sources. This is particularly beneficial for research, case management, and maintaining accurate client records. These instruments can analyze vast databases of information, extract relevant case law, and provide summaries.

With this development, routine workflows, such as approval processes, document reviews, and task assignments, can be automated to follow predefined sequences. Workflow mechanization guarantees that tasks are completed in a systematic and timely manner, lowering the chance of bottlenecks. Additionally, businesses exploring innovative payment solutions, like the option to “[buy USDT](https://paybis.com/buy-tether/)“, can seamlessly integrate such transactions into their automated workflows, ensuring efficiency and flexibility in financial operations.

Improved Due Diligence Processes

Due diligence processes, critical in various lawful contexts such as mergers and acquisitions, are undergoing a transformative evolution as well. AI algorithms can analyze financial records, contracts, and regulatory compliance documents, with speed and accuracy that surpass conventional manual methods. They can extract fundamental clauses, obligations, and deadlines, providing a detailed overview of contractual obligations. This streamlines the identification of potential issues and contributes to a more thorough due diligence assessment.

This development enables the visualization of complex data sets, offering intuitive means for decision support. It allows for a more comprehensive understanding of the relationships and patterns within the due diligence data. Also, it gives an opportunity to customize and tailor these processes to the specific needs of each transaction. This flexibility ensures that the efforts are focused on the most relevant aspects of the deal, optimizing the use of resources.

Automated procedures can cross-reference information across multiple sources, ensuring accuracy and verification. This capability is crucial in identifying discrepancies or inconsistencies in the information provided.

However, many users often wonder how to do [app development](https://wesoftyou.com/services/custom-software-development-company-in-new-york/) qualitatively. For this, you don’t need to spend a long time looking for good and trusted developers. You can simply turn to artificial intelligence, but it is important to ask the right question.

Challenges and Considerations

The adoption of automation technologies in legal practices brings about numerous advantages, but it is paramount to navigate the associated challenges. Specialists must approach it strategically. Below we gathered some of the issues you might encounter and the solutions you can apply.

Data Security and Privacy Concerns

Challenge: The handling of sensitive and confidential information raises concerns about data security and privacy.

Solution: Implement robust security measures, encryption protocols, and compliance with data protection regulations to safeguard client information.

Ethical Use of Automation

Challenge: Ensuring the ethical use of automation instruments, including transparency, accountability, and avoiding biases in algorithms.

Solution: Prioritize ethical considerations in the development and deployment of these technologies, adhering to professional standards and guidelines.

Adaptation and Training

Challenge: The successful integration of this innovation requires workers to adapt to new tools and workflows. To address the challenges of adapting to new technologies, organizations can leverage [ai development](https://www.apriorit.com/our-expertise/ai-machine-learning) services and expertise to streamline the integration of AI-powered solutions into their legal workflows and processes.

Solution: Invest in comprehensive training programs to ensure that legal teams can properly leverage all the tools, maximizing their benefits while minimizing the risk of errors.

Human Oversight

Challenge: Human oversight remains necessary, especially in interpreting nuanced legal issues and making strategic decisions.

Solution: Strike a balance between automation and human expertise, providing that all decisions incorporate legal judgment and ethical considerations.

Interoperability and Integration

Challenge: Integrating these implementations with existing systems and workflows can be challenging, leading to issues of interoperability.

Solution: Assess the compatibility of automation tools with their existing infrastructure and invest in solutions that easily integrate into their workflow.

Costs and Return on Investment

Challenge: Implementing these technologies may entail initial costs for software, training, and infrastructure upgrades.

Solution: Conduct a thorough cost-benefit analysis to determine the potential return on investment, considering both short-term and long-term gains.

User Acceptance

Challenge: Resistance to change and user acceptance may pose difficulties during the adoption of new developments.

Solution: Involve key stakeholders in the decision-making process, communicate the benefits of automation, and provide adequate support and training to enhance user acceptance.

Scalability

Challenge: Scalability issues may arise when expanding the initiatives to handle increased workloads.

Solution: Choose resolutions that are scalable and can adapt to the growing needs of the practice.

Bias and Fairness

Challenge: Ensuring fairness and avoiding biases in algorithms, particularly in AI applications, is a significant concern.

Solution: Assess and manage biases by promoting fairness and equity in decision-making processes.

Conclusion

The integration of Artificial Intelligence into legal practices represents a transformative shift that has far-reaching implications for this industry. The multifaceted impact of this innovation on legal research, document review, contract management, predictive analytics, automation of routine tasks, and due diligence processes underscores the profound changes. It is definitely reshaping the way legal professionals work. While offering unprecedented efficiencies, accuracy, and strategic insights, the adoption of AI also brings forth challenges.

They are related to ethics, data privacy, and the need for ongoing adaptation. A balanced and responsible approach to harnessing the potential of this technology will be paramount in ensuring the continued advancement and ethical practice within the legal field.

154. [Legal Technology & Alternative Legal Services Guideline](https://www.cyrilshroff.com/legaltech-als/)

Legal Technology & Alternative Legal Services

cam is the first Indian law firm to adopt Artificial Intelligence (AI) and Machine Learning (ML) based Legaltech in its day-to-day practice. The firm’s focus on driving innovation has resulted in the utilization of various AI and ML tools for tasks such as due diligence, contract review and abstraction, evidence management, litigation strategy, legal research, and intellectual property.  These tools leverage the firms existing practices and add value for our clients and practice groups. The use of Legaltech at the firm is not limited to one practice area or one technology. We focus on identifying challenges and exploring relevant solutions to increase efficiencies across practice areas.

Automated Proofreading and Editing

An integral part of a lawyer’s work is proofreading and editing drafts and documents. cam is committed to providing quality documents with the highest level of accuracy to its clients. The use of proofreading tools helps in:

Removing inconsistencies in usages and styles across a document;

Reducing time spent on manual search for errors;

Increasing efficiencies and accuracy, allowing Associates to focus on more high-value tasks.

Contract & Due Diligence Review

To support our practice groups with the due diligence process, we use an AI-based contract review tool. The tool helps our lawyers identify and quantify key risks, obligations, and deal breakers.  We have seen an average of 20% to 30% increase in efficiency using this software. We have identified various use cases for the tool at the firm, including Lease Review, Force Majeure Audits, Insurance Reviews, Contract Comparisons, Obligation and Change Management reviews. The General Corporate and Capital Markets practices benefit the most from this tool.

Client Focus: Through the use of this technology, we are able to gain actionable insights into deal points and advise our clients on future trends and risks.

Document Automation

Document automation uses technology to standardize document drafting. We currently use document automation as part of our internal quality assurance processes to standardize agreements.

Since automation maintains quality, consistency, timeliness, and cost efficiency while drafting various standard and complex documents, our lawyers are able to focus on complexities along with contract negotiations and overall strategy.

Client Focus: Through various projects, cam advises established clients as well as new businesses and startups towards standardizing their key documents and provides ongoing assistance in streamlining the document assembly process.

eDiscovery & Litigation Services

To complement the services of our Disputes team, we leverage eDiscovery technologies to effectively process and analyze high volumes of documents or e-files. We work with a range of eDiscovery platforms depending on the nature of each case. Our services offer end-to-end case and evidence management, including hosting, processing, and high-speed analysis of large data sets, using Technology Assisted Review or Predictive Coding. The team uses eDiscovery technologies to work on White Collar Crime Investigations, Government requests, Investigations, and Litigations including class action suits, Discovery Requests, etc.

These tools support the Disputes team by providing them the ability to:

Review matters end-to end;

Maintain Attorney – Client Privilege;

Identify and flag urgent information, even while the review is underway.

Legal Research & Litigation Strategy

By nature and training, most lawyers are thinkers and questioners. Over the years, we have used books and websites to research and analyze all possible angles of our arguments. Research methods have evolved and enhanced the capabilities of our Associates, through the adoption of various AI-based research tools to perform primary and secondary legal research.

These tools further enrich the firm’s service offering to clients, which are as follows:

Providing more accurate and relevant search results at optimum speed;

Increasing time efficiencies and saving cost by using the best technology to assist Associates to analyze their research.

Ability to quickly and granularly map case law and assess relevance;

Centralized management of case-related tasks and reminders;

Improved efficiencies by providing more sophisticated and accurate search results, which are not merely based on keywords;

Reduction in hours spent on understanding the relevance of a case law to the matter;

Early identification of possible counter arguments, informing case strategy from the initial stages of a dispute.

155. [AI workplace use policu](https://www.rocketlawyer.com/business-and-contracts/employers-and-hr/company-policies/document/ai-workplace-use-policy)

What is an AI Workplace Use Policy?

An AI Workplace Use Policy is a set of guidelines and rules established by a company to govern the appropriate and responsible use of artificial intelligence (AI) technologies in the workplace. With the burgeoning use of generative AI in both work and personal settings, having an AI policy in place that defines the risks and appropriate uses of the technology for work purposes can help to mitigate potential risks to the company itself.  
  
AI Workplace Use Policies outline the expectations, rights, and responsibilities of both employees and the company regarding the use of AI tools and systems. The policy covers permitted uses of AI, requesting permission, both the employee’s and company’s obligations, intellectual property issues, data privacy and protection, and protection of confidential information.

When to use an AI Workplace Use Policy:

You’re an employer who wants to ensure employees follow established guidelines for proper use of artificial intelligence in the workplace and understand the risks to the business of using the technology in a reckless manner.

You’re a business owner who wants to implement AI policies in your company to assure clients that you are taking seriously the risks associated with AI use.

Workplace AI Use Policy checklist

Complete your free Workplace AI Use Policy with our Make it Legal™ checklist

Make this document

Customize your Workplace AI Use Policy by answering simple questions. We’ll help you along the way and build a document that fits your needs. Plus, you can always save and continue later once you’ve started your document creation process. [Get started now!](https://www.rocketlawyer.com/StartDocument.aspx?id=2648&try=1)

Review your policy

Look over the Workplace AI Use Policy to ensure it matches your intentions. If you need to make changes to the Policy outside of the interview, you will be able to make changes online or in Word format in the Document Manager at the end of the process.   
  
Remember that if you have any questions you can easily [Ask a Lawyer](https://www.rocketlawyer.com/legal-advice).

Distribute

Provide a copy to each employee. Add the Workplace AI Use Policy as an attachment to your Employee Handbook for future reference and for all new employees.  
  
Keep a copy of all documents for your own records and in case there is a problem.  
  
You can use Rocket Lawyer to store your Workplace AI Use Policy. Safe and secure in your Rocket Lawyer account, you can access it anytime from any computer, as well as share it for future reference.

Purpose of the AI Policy (“Company”) is excited by opportunities for innovation and efficiency offered by artificial intelligence (AI) models and tools. We inted to incorporate AI into our Company’s operations in a safe, ethnical, and legally compliant manner. We aim to enable our Company, employees, and other stakeholders (e.g., our clients0 to obtain maximum benefits form new and established AI technologies.

The Company has implemented this AI Workplace Use Policy to help us to achieve the above

Reasons to Update

To add, change or remove which AI tools and use cases are permitted.

To add, change or remove which user groups may use the tools.

To add, change or remove who will be responsible to review and approve AI integrations.

To provide additional rules for use of AI or clarify information previously provided.

156. [Artificial Intelligence Use Case at A&O](https://www.allenovery.com/en-gb/global/expertise/practices/artificial-intelligence)

In February 2023 our team became the first in the world to implement generative AI across an international law firm at enterprise level.

Thousands of our lawyers in 43 jurisdictions now use GPT-4-based tools in their day-to-day work.

Pioneers in the use of generative AI

Our client advice is grounded in the extensive and rigorous program we undertook to safely and responsibly integrate this technology – Harvey – in our own business.

And we don’t just use AI-based tools, we build them, too. Our proprietary contract drafting tool, [ContractMatrix](https://www.aoshearman.com/en/expertise/markets-innovation-group/contractmatrix) – developed in partnership with Microsoft and Harvey – streamlines contract drafting, review and analysis.

ContractMatrix has been tested and refined by more than 1,000 of our lawyers and, following its launch at the end of 2023, is now being licenced to clients.

We understand all forms of AI and the specific issues each raises from a risk management, contract and licencing perspective.

Our experience spans everything from helping nation states shape their AI policies to advising businesses across industries on how to develop effective and responsible AI solutions, handle AI-focused transactions (including M&A, JVs and collaboration deals), construct AI collaboration agreements and manage AI-related disputes.

[They are] miles ahead of any other firm on AI.

Representative matters

A syndicate of global organisations on the safe deployment of generative AI. Our work included developing a toolkit for assessing and mitigating key legal risks (across U.S., U.K. and EU laws) and implementing an enterprise change management programme to support the deployment of generative AI.

A life sciences company on the design and drafting of a governance framework to triage AI use cases across its global functions and businesses, as well as building the software application to encode that framework .

Sole legal counsel to Partnership on AI; advised on its draft generative AI safety protocols and a collaboration arrangement relating to the roll-out of certain of its data ethics guidelines.

A provider of metaverse solutions on compliance with data protection law and the new digital EU regulations.

A global IT services provider on a global compliance programme for the use of generative AI.

A private equity fund on the strategic issues arising from the development of generative AI models.

Leading AI drug discovery company Exscientia on its c. USD700 million collaboration agreement with Merck for the deployment of Exscientia’s AI platform.

A government on its roadmap for adoption of AI across various g

HARVEY

Our deployment of Harvey, an OpenAI-backed tool based on GPT-4, began with a sandbox. In other words, we gave access to a limited number of lawyers in a ring-fenced environment. Sandboxes are crucial for any business looking to deploy generative AI because it’s hard to predict what the technology will do until you use it. We tested, adapted, and moved ahead – all in a safe and secure environment. We only rolled out Harvey to a wider group once we could mitigate its risks, and we continue to gather and act on feedback we receive.

We also established an AI steering committee and an AI brains trust to help our experts understand AI’s current and future capabilities and how it can be harnessed across every area of our business. Alongside this, all our existing governance structures, including our risk committee, now consider generative AI in their day-to-day decisions.

Clear governance and guardrails are critical to successfully deploying AI. We have specific rules of use in place and train our people how to use AI tools effectively and safely.

People are the common thread that runs through all our work with AI. We know that generative AI is an augmentative tool. Everything Harvey produces is rigorously checked, edited and finessed by our team. It enhances the work our lawyers do and helps us produce better results for our clients. In turn, it is governed and augmented by the gold-standard critical thinking and creativity for which A&O Shearman lawyers are known.

OUR AI GROUP

Our multidisciplinary AI Group advises clients on the responsible development, deployment and use of AI.

We combine a sophisticated understanding and experience of technology with deep expertise in intellectual property, data privacy, regulation, technology transactions, litigation and change management.

We help our clients to manage the risks associated with this powerful technology which fall under two broad categories.

First, AI models make errors. Crucially, even those who build and train the models can’t explain and account for them. This so-called “black box” problem creates significant risks.

Hallucinations: These are incorrect outputs that could lead to, for example, tort liabilities, consumer harm or regulatory breaches. Hallucinations can be the result of incorrect or out-of-date data, inaccurate mathematical predictions based on weighting of sources or randomization, or historical bias in the datasets used to train the models.

Unpredictability: A lack of explainability also creates a lack of predictability: you can’t be certain exactly what the model will say in response to a question. This can make it extremely difficult to check that it meets standards of quality and accountability.

Response divergence: By their very nature, AI models will give multiple answers to the same question. This could be evidentially relevant if, for example, an AI chatbot built to give financial advice delivers different responses to two individuals leading to divergent outcomes.

Second, generative AI models take human content and account for it in a mathematic response. A user may therefore be working with someone else’s information without permission, credit, knowledge, or even awareness. This raises significant IP infringement questions: for example, can the user assert ownership over the model’s output? And is their own IP safe if they are using the model?

There are also consequential questions about data privacy and data protection, for example, where an AI model has been trained using personal data or a user inputs personal data as a prompt.

Our AI Group provides answers to these substantive legal questions on a syndicated basis. You can sign up to join a series of one-hour calls with other businesses, each in a controlled environment monitored by an antitrust lawyer. The calls deal with specific issues and are supplemented by minutes and additional written materials such as formal memos, policy guidelines, or comparative analyses.

So far, we have covered topics including a primer on AI, ChatGPT policy, IP infringement and data risks, licensing a large language model (LLM) and change management, and have welcomed attendees from industries including financial services, pharma, technology and telecoms.

For more information, please get in touch with your usual A&O Shearman contact.

CONTRACTMATRIX

At A&O, we don’t just use AI-based tools: we build them.

[ContractMatrix](https://www.aoshearman.com/en/expertise/markets-innovation-group/contractmatrix) streamlines contract drafting, review and analysis using:

Generative AI-assisted interrogation and drafting

Real-time access to your gold-standard precedents and policies

Inbuilt risk management and governance designed by A&O Shearman lawyers

It has been developed in partnership with Microsoft and Harvey, which builds custom LLMs for lawyers. ContractMatrix has been tested and perfected by more than 1,000 of our lawyers and, following launch at the end of 2023 with [Financial Times coverage](https://www.ft.com/content/f1aff4d0-b2c5-4266-aa0a-604ef14894bb), is now being licenced to clients.

157. [Good practices using AI](https://www.demarest.com.br/wp-content/uploads/2022/01/DEMAREST_Good_Practices_IA_EN.pdf)

Artificial Intelligence (AI) is already a reality whose uses and benefits are apparent both for individuals and organizations. It is present in our daily lives and in our vocabulary and its countless utilities and applications become incrementally clearer. The use of chatbots, which help users with questions related to products and services, and virtual assistants, which perform tasks in response to commands and offer several types of assistance, are examples of the use of technology that benefit both the companies and the users. According to a 2021 survey conducted by IBM1 , one third of the information technology (IT) professionals surveyed stated that their companies already use AI. The data also indicate that 74% of the companies are exploring or using the technology and that they have accelerated the implementation process due to the COVID-19 pandemic. Despite this, the topic is not always discussed based on a clear concept of what AI really is, and ethical-legal aspects already consolidated in the local and international scenarios are also not considered in their entirety. There are ethical principles that underlie the use of this technology, which must be observed from the moment of creation to its practical application. That is the case, for example, of the principle of nonmaleficence, which, in general terms, establishes that Artificial Intelligence should be used without causing foreseeable and intentional damage, as well as establishing that risks should be mapped and, as far as possible, avoided. It is not uncommon that the debate on AI and even its application is not accompanied by a clear conceptualization, which is important to defining the applicable ethical-legal system, differentiating it from other technologies.. In general terms, we can say that Artificial Intelligence consists of algorithms trained by data to perform certain tasks autonomously – tasks that, until then, could only be performed by human beings. Hence, human intelligence and Artificial Intelligence are complementary. After the programming of the machine, however, AI is often able to independently perform tasks such as analyzing databases, identifying patterns and recognizing faces and objects. On the one hand, AI is, as many people presume it to be, complex. Choosing mathematical I models and architectures of well-known artificial neural networks requires specialized technical knowledge. On the other hand, however, it is extremely practical, intelligible and applicable. Once created, its use can be simple. Thus, this technology is very useful and provides countless advantages to the companies, such as reducing production time and costs, bringing clients closer and increasing productivity, aspects that, when combined, generate high economic impacts. In recent decades, we have witnessed an intense digital transformation, which has grown even further in recent years with the use of algorithms and their derivations. This has led several organizations and companies to dedicate themselves to business transformation by integrating new technologies into their operations. This commercial and digital transformation has also been positive for attracting new consumers, who seek services and products adapted to the new reality. The levels of demand, publicity and public scrutiny to which companies are subject require processes that respect ethical tenets and legal rules. A company with processes adapted to local and international standards for the use of Artificial Intelligence also tends to attract more qualified professionals, creating a circle of generation of benefits for all parties involved. Companies improve their processes, products and services by applying technology in an ethically responsible manner; consumers have access to better quality products and services; professionals work in establishments that respect the existing rules in order to provide better services and seek companies that are in accordance with their level of qualification; finally, in this cycle, companies attract more consumers, increase sales figures and arouse the interest for collaboration from even more qualified professionals. In addition, there is also the possibility of establishing commercial partnerships, whether at the local or international level, with companies equally adapted to new technologies and concerned with ethical-legal issues related to their use. In this regard, McKinsey Global Institute emphasizes that AI has great potential to contribute to economic activity around the world. It is estimated that by 2030 the technology will add 13 trillion dollars to economic production, with a 1.2% increase of the annual global GDP2 . Despite all of these potential benefits, integrating Artificial Intelligence into a company’s routine is not a trivial task and cannot be done in a careless or hasty manner. While the introduction of AI can bring major advantages, its careless use carries high risks. In other words, what is a great opportunity for growth can also be a threat and generate conflicts from the perspective of civil liability. This leads us, once again, to the need for knowledge and practical observance of the ethical-legal standards that govern Artificial Intelligence in all processes and stages of application in a company. In general, it is necessary to take a preventive stance, attentive to possible risks and adopting measures to avoid them before they manifest. Accordingly, the ethical and responsible use of AI will ward off the main risks of its use and reinforce its potential. As happened with the Brazilian General Data Protection Law (LGPD - Law no. 13,079/2018), which resulted in the mobilization of companies to adapt to the legal requirements related to the protection of personal data, Artificial Intelligence will soon be on the agenda of several organizations, which will seek its integration into their processes and adaptation to the legal regulations. Hence, companies that take notice of the technology’s growing momentum, which is already apparent to the more attentive observer, will be able to define, in advance, measures to understand the ethical-legal contours and parameters of the technology and the ways in which it can be incorporated into their business. In a short time, these measures will constitute the grounds for a great competitive differential. Within this context, the purpose of this Guide is to provide a comprehensive introduction to Artificial Intelligence, addressing its concept, the principles and rules involved and the consequences of its use. The approach used here is aimed at the practical application of the technology, focusing on serving as an aid for companies that are willing to implement it in their products. Thus, we seek to provide guidelines for the ethical and responsible use of AI, intensifying its potential applications and ensuring compliance with mandatory measures. To achieve this purpose, we begin this Guide with a detailed explanation of Artificial Intelligence. In chapter 1, we address the concept of technology, its characteristics and modalities. Next, we present and explain the principles that must be observed for an ethical, responsible and reliable use of AI. Item 3 deals with AI compliance, commenting on the main local and international rules that dictate the use of the technology. Complementing this topic, in item 4 we discuss the relationship between Artificial Intelligence and data protection, which gives rise to the application of specific rules, including requirements of cybersecurity, and on the relationship between AI and Intellectual Property (IP). Following this, there are some recommendations and best practices to be followed by companies that already use or want to use AI in their processes. These encompass concrete measures that are intended to meet legal and ethical requirements and which reinforce the logic of risk mitigation. In item 6, we briefly present some success cases in the use of the technology that indicate its potential. This content is followed by a list of steps to be followed by companies: a brief summary focused on the practical and actionable steps that can be carried out by organizations. To conclude this Guide, we indicate some glossaries for consulting common concepts and expressions in the field of AI, in addition to the references used, which can also be consulted for further in-depth study Although it is possible to indicate more remote origins and significant groundwork related to Artificial Intelligence, it was mainly since the 1950s that the concept began to assume a format closer to how we conceive it today. There are two fundamental milestones that paved the way for the concept: the Turing Test and the conceptualization of John McCarthy. Alan Turing, in an article published in 19503 , described his experiment which became known as the Turing Test or the imitation game. In general terms, it refers to running some tests in which a human being and a computer should provide answers, and, in the sequence, another human being would analyze them and attempt to distinguish which were given by the machine. If the distinction is not possible, the machine is said to have passed the test. The test was enthusiastically received by the scientific community, which began to explore the idea and experiments even further. A few years later, in 1956, a seminar lasting about two months was held at Dartmouth College in New Hampshire, in the United States, where scientists, who would become the most instrumental for AI, met to discuss various issues that were on the agenda at the time, such as the limits and possibilities of machines’ capacity and their potential to perform tasks until then performed only by humans4 . The pioneering use of the expression Artificial Intelligence was made during this seminar by John McCarthy. Following these contributions, the topic became more present on the agenda of scientists, and debates, experiments and events were dedicated to testing and developing the capacity of machines until we reached the current state of evolution5 . Even with countless studies and discussions, there is still no universal concept of Artificial Intelligence. However, it is possible to deduce the common idea between the different concepts, which allows us to clearly understand what we are talking about, when referring to AI. In general terms, Artificial Intelligence is the term used to designate systems that have the capacity to learn and perform tasks previously only performed by humans. As a rule, this execution is preceded by the development and training of algorithms6 carried out by a person, but there are already artificial intelligence systems that have the capacity to learn on their own as they carry out their activities. Models and algorithms have improved exponentially and performed increasingly complex tasks. There is an important AI feature that contributes to this development: the technology is based on the use of data – in general, a large volume of data, known as big data. These data feed the Artificial Intelligence, allowing for more accurate and informed decision-making. It is based on such data that different AI functions are performed, such as sorting data, generating forecasts, identifying and sorting images, making decisions, and many others7 . These are things that, until the advent of AI, only humans have been able to perform. Similarly, Luciano Floridi and Josh Cowls present a concept of AI that, despite having debatable aspects, allows a clear understanding of the theme and documents referring to technology The concepts of Nils Nilsson and Nick Bostrom also help with the more comprehensive understanding of what exactly is being referred to when talking about AI: Due to the fast-paced technical evolution that AI is providing and will provide in the near future, it has even been said that its potential will surpass human intelligence. However, as we have already mentioned, there is an understanding that it is unfeasible to talk of replacing one intelligence with another. It is, in fact, a relationship of connection and complementarity. By performing even simple tasks, AI is already contributing to allow the human brain to focus on more difficult and complex issues that machines cannot yet perform, and even to develop machines with ever-greater capabilities. Thus, Artificial Intelligence will even enhance human capabilities and perform tasks that the human brain alone cannot – or that can carry out at a much lower speed. This may seem difficult to grasp, but we can think, for example, of a comparison between the human memory capacity, which is limited and tends to degrade over time, in relation to the storage capacity of a computer, whose data, if treated properly, will not degrade and storage is virtually unlimited. Similarly, AI is capable of processing a greater amount of information at an even greater speed. However, it is worth emphasizing once again that these feats are only possible, at least currently, as a result of human collaboration, which reinforces their complementary nature. Today, AI shows a great deal of potential in specific applications that are already widely used in our daily lives. This Artificial Intelligence that we currently use is referred to as Weak or Narrow AI, due to its limited ability to perform functions other than those for which it was trained. There is, however, an expectation regarding what has been categorized as Strong or General AI, but we still do not know how or when this will become a reality. “Weak Artificial Intelligence (Weak AI or Narrow AI) is a specific intelligence, focused on an activity or area and that performs only that for which it was taught. It is the classic example of the system programmed to play chess, which plays only chess, but does it with excellence. It is the most used form today and is more present in our daily lives. The fact that it is called weak, however, does not diminish its unprecedented utility to perform complex tasks, and to learn from the data and contexts it is given. This is the case, for example, of recommendation algorithms, chatbots and even autonomous cars. In turn, Strong Artificial Intelligence or General Artificial Intelligence11 is not limited to a specific issue, given that it possesses a more general and comprehensive intelligence, adapting to different contexts and situations. Due to its complexity, it has yet to be developed and will require greater attention due to the risks it can generate. Below, we present an outline of the main learning techniques involved in training Artificial Intelligence algorithms, in order to understand how Machine Learning works. Machine Learning With this method, the algorithm is trained with a large amount of data in order to answer questions and solve problems. Among the most used algorithms in machine learning are “decision trees”, “K-means” and “deep learning” to solve tasks that can vary between “supervised learning”, “unsupervised learning” and “learning by reinforcement”. What makes Deep Learning attractive is its ability to solve all three tasks, as explained below. Supervised learning The most utilized technique today. It uses data labeled by humans for training and for testing the results to verify that the algorithm generates responses with the expected accuracy. With this technique it is possible, for example, to make forecasts, such as sales in a given scenario; analyze probabilities; sort images and other data. 1. Unsupervised Learning Uses unlabeled data to explore possible results, seeking information that, a priori, is not known. Through, for example, grouping (according to client profile, behavior, etc.) and data associations, it generates useful results for the company, such as identifying patterns and problems. 2. Learning by reinforcement Uses positive and negative reinforcements and uses its own mistakes and successes throughout the process to learn how to make a decision/choose the best path to follow. It can be used, for example, to recommend content and advertising: depending on whether a client consumes the recommended content and the products indicated, the algorithm learns more about the client’s preferences. 3. Deep Learning12 This is a more sophisticated form of machine learning, which learns and performs more complex tasks. Based on neural networks, which are inspired by the functioning of the human brain, they use a large number of artificial neurons connected in multiple layers, hence the reference to their “deep” nature. Its configuration can be carried out mainly through 3 different machine learning tasks: Natural Language Processing (NLP): the area that is dedicated to linguistic processing, recognizing meanings in texts and speech, allowing communication with humans. This technique is widely used in Chatbots, translators and virtual assistants like Siri, Alexa, Google Home. Robotic process automation (RPA): as the name suggests, it refers to the automation of certain tasks and processes, which can involve different files and even systems. For example: filling in documents, reports and spreadsheet data; copying data between and among forms; detecting payment for subsequent issuance of invoice, followed by shipment of the product; and organizing registrations. It is useful for mechanical processes, which traditionally are done manually and in which there is practically no variation. It is an attractive alternative for starting the application of AI in a company, as it does not require major structural changes or an extremely advanced IT infrastructure. Chatbots: the algorithms are programmed to, from their database, allow the machine to interact and converse with humans, either through voice or text. It is one of the easiest applications to understand and it can be used for customer service, FAQ and even to schedule services. It can be used in combination with other AI techniques, enhancing its effect. Along with NLP, for example, the chatbot becomes able to understand more clearly what the user means. With machine learning, the chatbot learns from conversations, improving its responses. Recommendation algorithm: an algorithm that makes recommendations for content, products and services based on users’ profiles. The algorithm needs to be fed with data, which will be categorized to identify patterns with cutouts, for example, of gender, age and social class. Based on this, it will analyze, depending on the case, consumption habits, consumed content and the like to make new recommendations. To keep up to date, the algorithm requires considerable data storage and processing capacity. This is what we see, for example, in movie, series and music streaming apps, as well as social networks recommending new content and stores that potentially will be of interest to the user. The use of this algorithm by a company allows a more precise reach of its target audience, but it must be used with caution – both during its preparation and feeding with data and when presenting recommendations to clients, as insistent contact, poorly directed or without clear consent in data collection can generate discomfort and alienate the client. The algorithm can be enhanced with the crossing of AI technologies, especially machine learning. All of these techniques provide, as already mentioned, countless applications and bring several advantages to companies that use them, such as efficiency, due to: the low margin of error of the technologies; reduction of labor, especially in mechanical tasks, which can be done by a machine; standardization of processes and communication with clients; improvement of products and services; and through attracting new clients and more qualified Computer vision: the name itself denotes its concept, which is to give vision to a machine so that it becomes able to see certain things. It is used to recognize images and videos and extract data, patterns and the like from them. A practical and widely used example is facial recognition. professionals. Among its applications, we mention only for illustrative purposes: the referred chatbots; the use of algorithms to recruit professionals and select candidates with a profile closest to that sought; employee and company performance analysis; recommendation of content, products and services to users and clients; value forecasting and market analysis; credit analysis; traffic management and indication of alternative routes; decisionmaking; applications in smart homes; assistance in medical diagnosis; image recognition and biometrics; verification of identity and veracity of documents; autonomous vehicles; prevention of process failures. Note that these applications may demand and/or benefit from the use of other technologies that are not to be confused with AI, but which mutually enhance the potential. This is the case, for example, of drones, the Internet of Things and wearable devices. These are technologies that inevitably demand new and more complex processes, moreover because they considerably increase data production and touch on new privacy issues. In any case, all Artificial Intelligence requires specific due care and must follow rules that are already circulated locally and internationally. As the benefits of AI grow, the associated risks also accumulate. Many consequences of such risks can be anticipated and avoided in advance, but those that are unforeseen still exist, and action must be taken to avoid and minimize the damage. Thus, the use of AI should be made within a specific ethical framework and legal regulations, points that will be explored in the topics further below. The various applications of Artificial Intelligence bring unprecedented ethical challenges to human beings. This is amplified by the fact that the technology is relatively recent and is evolving at a rapid pace, including its high potential to change the way we live, impacting all areas of human life. Some of its ethical risks involve, for example, the proliferation of social stigma, the perpetration of fraud and disrespect for individuals’ rights. Consider, for example, the possibility of attributing to the machine the decisionmaking process that would have social and collective impacts, as would be the case with its use in public institutions. There are even consequences of current applications that are not yet foreseen, mainly due to the difficulty of understanding and controlling an algorithm in its entirety, as well as the existence of applications that we are not yet aware of, but which already raise moral concerns. As highlighted by Nick Bostrom and Eliezer Yudkowsky13, the ethical issues of Artificial Intelligence, especially strong AI, differ from those existing in relation to other non-cognitive technologies, because: 1) even if its configuration and training are done properly, the result may not be fully predictable; 2) checking the system security is a challenge, as it must be done in all possible contexts in which AI can be applied; and 3) the ethical concern must also be a concern of the engineering area. There are already debates about the moral status of Artificial Intelligence itself. The cognitive capacity that the system may have (which allows autonomous decision-making, learning and development independent of human intervention), raises the question of whether these machines should be considered themselves as moral beings14. In addition, ethical concerns about Artificial Intelligence also focus on the fact that its various applications can be used for the benefit of society, companies and citizens, but can also be used for harm. For these reasons, scholars on the theme, companies, international organizations and other important players in the field have indicated the need to observe ethical standards in the use of Artificial Intelligence. Today, some comprehensive ethical standards have already been developed and disseminated to create general limits for the use of AI. These are principles that have developed over the years and have contributed to delineating the limits and possibilities of applying AI and self-regulation, which are common in this field. Some companies, especially technology giants and global entities, already have solid Artificial Intelligence policies, which include a strong reference to principles. This is the case, for example, with Microsoft15, Google16 and the Organization for Economic Cooperation and Development (OCDE)17. Thus, there are principles and good ethical practices that are disseminated and accepted by the international community. These principles serve as the basis for the development of company policies, laws and guidelines from international organizations and for legislative discussion. In these policies and in laws already published on the subject matter, it is possible to notice the strong character of principles. There is actually a proliferation of principles, and each author and company treats them in a certain way. However, more in-depth analysis of these various principles allows us to identify that the multiple concepts all contain similar ideas. The concern, in general, is to make Artificial Intelligence responsible, transparent and, above all, trustworthy. Given the linearity of the logic underlying them, it is possible to group them into five general principles that should guide the use of Artificial Intelligence18, which are presented below. It should be noted at the outset that behind each of these principles are the notions of promoting human values and mitigating harm, putting the human at the center of the technology’s applications. Before analyzing each of these ethical principles, it is important to highlight that they should be observed in all phases of AI use, from the formulation of ideas and project design, through systems architecture, programming and engineering, to its practical application and possible subsequent consequences, which leads us to the notion of ethics by design19. This requires, among other things, a multidisciplinary and diverse team, as will be discussed later, and whose training covers ethical issues, including for engineers, programmers and the like. Finally, we add that the use of AI and the respect for principles should not be based on a passive stance of avoiding risks and biases. In other words, it is not enough just to program without biases or to believe that the security of the system itself guarantees that risks and damages will not occur20. Below, we will briefly explain what each of the principles consists of 2.1. Beneficence The principle of beneficence indicates, in general terms, that Artificial Intelligence must be used in a beneficial way for humanity. Thus, it must be focused on the well-being of human beings, empowering as many people as possible, respecting human dignity and also being attentive to the sustainability of the planet21. In summary, it can be translated into the idea of doing only good. 2.2. Non-maleficence The principle of non-maleficence can be translated, in few words, into the idea that the use of AI should not cause harm. Thus, its misuse should be avoided, as would be the case of using it in an arms race. The development and application of AI technology should only occur within the limits of safety, and should prevent not only the violation of privacy, but also other fundamental rights. This principle also involves the assumption of the responsibility for working against possible technology risks22. 2.3. Autonomy The principle of autonomy seeks to emphasize that the Artificial Intelligence should be used in a way that it does not weaken or annihilate human autonomy, but that should, on the contrary, promote it. When using technology, we give the machine a certain power of decision, but this needs to be done in a balanced way, that is, balancing the power delegated to the machine and the power maintained by us. Furthermore, the power to delegate decisions and to withdraw that delegation must always be held by humans. Otherwise, there is a risk that AI autonomy will undermine human autonomy. Based on these ideas, Floridi and Cowls refer to a “targetautonomy” or “decide-delegate” model23. 2.4. Justice The principle of justice is based on the idea that there is inequality of autonomy in society and, therefore, AI should be used to promote justice. It is a principle broadly addressed in different documents and varies according to the authors, but, in general, it indicates the need to eliminate any type of discrimination in the use and results of AI, in addition to promoting aspects such as prosperity, solidarity, justice, equity, diversity and equal access to benefits in society24. One of the consequences of the principle of justice, especially in terms of non-discrimination and absence of prejudice, is the non-existence of biases throughout the processes and, above all, in the results. Biases in AI can be defined as a biased and disproportionate analysis that disadvantages a person or a group. Take as an example the AI credit analysis, which, in some cases, has generated discriminatory results: credit denied for reasons of race and geographic location, to the extent that black people and people living in poorer neighborhoods had their requests denied, even if, initially, the AI was not intentionally configured to make a decision based on these factors. As observed by Dora Kaufman25, these errors may occur: before data collection, due to programmers’ decisions; in the data itself, which occurs in the event that the data are not representative and proportional to the portion of the population to which it refers; still in the data itself, but reproducing prejudices that exist in society; and also due to labeling errors (prior to supervised learning) or in data generation. In this way, the importance of the existence of diversity in the data and of adequate categorization and selection becomes clear. Otherwise, the decisions of the algorithm will reproduce the human biases already present, usually unconsciously, in the implementation and feeding of the technology. As we have already highlighted above, overcoming biases is not possible if a certain factor is ignored: a positive action is necessary for the algorithm to understand that some factors should not be regarded in a negative sense in the decision-making. Once the AI system has been fed with data, it might be difficult to identify the source of the bias. Algorithm auditing, which will be covered in this Guide, can be fundamental in this process of recognition and overcoming of bias. 2.5. Explicability The principle of explicability complements and reinforces the four principles observed so far26 and it can be divided into two main ideas: intelligibility and accountability, as explained by Floridi and Cowls. Intelligibility is concerned with how the AI system works. Thus, it is necessary to have transparency and the possibility of understanding, interpreting and explaining how the decision-making process works. Accountability is concerned with who is responsible for the way the system works. This principle of explicability is strongly related to the attempt that has intensified in recent years to reduce the black box aspect of algorithms, which is connected to the “lack of understanding of how the so-called data inputs generates the output data, how the system correlates the variables contained in the input data and the assigned weights (called ‘parameters’)”27. Thus, as Dora Kaufman observes, the purpose is to understand and transmit in a clear and accessible manner to the user how the system reached a certain result. It happens that accuracy and transparency are inversely proportional factors in AI systems, which still represents a challenge for programmers. This becomes even more real, according to the complexity of systems: processes based on deep learning, for example, become increasingly harder to explain. In short, explicability, especially in terms of transparency, requires clear communication, through an accessible language to the consumer, and it is also recommended to use specific tools whenever possible28. Project traceability is also required, in order to be able to define what was done at each stage and throughout the entire process to explain the system and its decision-making to the user. As already observed, it is increasingly clear that AI will significantly change the way we live. The forecasts point to great impacts in all areas of life, with emphasis on the social, cultural and economic aspects. Technology can impact lifestyle, private choices and political decisions29. Thus, ethical principles that delimit both the use of Artificial Intelligence and the legal aspects become even more important. In Europe, for example, a trend towards the regulation of technology has been observed and, as happened with the LGPD, which was inspired by the European Union’s General Data Protection Regulation (GDPR), we believe that the treatment of AI in Brazil will follow a similar path. It was mainly from the 2000s onwards that saw stronger investment in this technology30, causing it to develop at a faster pace. Over time, the potential of AI and its commercialization became increasingly real, but the discussion on regulation of AI only started to advance relatively recently. However, regulating technology is not an easy task, especially one such as Artificial Intelligence, which is evolving at a rapid pace, resulting in an equally rapid obsolescence and insufficiency of laws, and that will have even more profound impacts on society and the economy. While seeking to protect rights and values, it is necessary to leave room for technological development. However, it is unfeasible to presuppose a total dichotomy between innovation and legal treatment or the idea that the legislation would create barriers to economic progress. It is necessary and it is possible to find a balance. Many times, the adoption of similar principles and rules – whether from a state regulation or a self-regulation of industries and companies – enhances the attraction of investments, as it ensures a suitable environment for business development, protects Intellectual Property and individual rights. In light of this, what has in fact been observed is a greater rate of the proliferation of principles, the self-regulation of large technology companies and the establishment of policies by international entities, aspects addressed in the preceding item. We can also observe an increase of debates, proposal and discussion of bills, public forums, initiatives of working groups and research laboratories and other measures aimed at developing an efficient state regulation. The debate is more advanced, especially in developed countries, but there are still countries that find themselves in a scenario of insufficient legislation on the subject. This is the case of Brazil, which does not yet have a specific law addressing the use of Artificial Intelligence, but the discussion has been already been initiated and is expected still to expand, within the scope of discussions in society, the legislative and executive branches, the public sphere and among the entities and authorities interested in the discussion. Note that the discussion here is carried out considering specific rules on Artificial Intelligence and, in some cases, more comprehensive rules related to digital law. Nonetheless, this does not exclude the need to observe other rules also applicable, such as those of Intellectual Property, competition law, civil liability, consumer law, among other local and international legal rules. Due to the innumerous possibilities of using Artificial Intelligence, many other rules are mandatory depending on the case and the area of operation, as seen in the insurance, medical, pharmaceutical and financial areas. Therefore, we present below a general overview of the Brazilian and international scenarios for the regulation of Artificial Intelligence. As we shall see, a common point of the rules is to seek to ensure enforcement of ethical principles, guarantee respect for the rights of users, delimit the possibilities of using the technology and minimize risks. Note, however, that although some countries do not have laws on the subject and others have more general laws, this does not prevent the use of AI. On the one hand, the law itself establishes general principles and rules that already present the direction and delimitation of what must be done and what is prohibited in the use of the technology. This is the case, for example, of the constitutional principles, which prohibit discrimination and ensure the protection of honor and image, and also other laws that address the issue, such as the LGPD and the Brazilian Internet Civil Framework. On the other hand, although the trend has been to regulate AI, this does not prevent companies from acting proactively to create their own rules and good practices to align their operations with the best standards of the market and compliance. After all, regulation, especially of a technology, does not operate solely in a top-down movement, in which the State creates laws to be followed by companies. Companies themselves can be proactive in this context, creatingv 3.1. The Brazilian scenario As mentioned, we still do not have in Brazil a specific law addressing Artificial Intelligence and even the bills of law on the subject are recent, proposed from 2019 onwards33. Among these, Bill PL 21/2020, proposed in the House of Representatives, has gained some prominence in the national debate. The Bill “establishes foundations, principles and guidelines for the development and application of Artificial Intelligence in Brazil”. Throughout its articles, the Bill deals, among other things, with conceptualizations of important issues for Artificial Intelligence; introduces fundamentals for the use of AI, listing aspects that should be promoted with such use; presents the principles to be observed for responsible use of AI, which approach the aspects mentioned in item 2 of this Guide and also principles already established in the area of data protection. The other bills already proposed so far follow similar paths, despite having important differences. Mateus Fornasier and Norberto Knebel34 note that such bills corroborate the trend towards social auditability of algorithms (accountability), indicating that algorithms must be justified in light of open and verifiable principles. The authors also state that the bills, in a way, reinforce the trend of self-regulation by the companies, as was seen with the LGPD, which, in its Article 50, provides that controllers and operators “may formulate rules of good practices and governance” in line with the principles and rules of law. Thus, in the context of AI regulation, “developers and operators are inserted in this same context of regulatory entity, at the internal level, both upon creating the systems and in their activities, enshrines the reality of regulation by design, that is, that the developers themselves are also responsible for the preservation of public order principles”35. Legislative activity in the country generated a reaction from the Executive Branch, which also adopted some initiatives with the aim of regulating Artificial Intelligence. This was the case, for example, of the public consultation of the Ministry of Science, Technology and Innovation (MCTIC) on the Brazilian strategy for Artificial Intelligence36 and the call to fund research centers for allocation in AI37. In 2021, the Brazilian Strategy for Artificial Intelligence (EBIA) (Ordinance GM No. 4617/2021, modified by Ordinance MCT No. 4979/2021) was published. However, in addition to the restricted scope of the EBIA, which provides guidance only to the Federal Government, its laconic forecasts do not resolve several doubts and issues that exist in the country. Although it is an important measure and presents concerns such as the elaboration of ethical principles and standards, the promotion of investments in research and development in the field and provides, for example, that AI should benefit people and the planet, the Strategy was received with criticism by AI scholars. In this regard, it should be observed that the document arrived late, presents a level of maturity below expectations, especially in comparison with the plans of other countries, and attributes few roles to the government itself in the sense of innovating in AI38. The document also lacks concreteness, as it does not contain clear responsibilities or budgetary considerations. The legal vacuum and legislative uncertainties, however, are not reasons enough to prevent the use of the technology in the country. Companies and organizations often create their own policies delimiting the parameters of AI (self-regulation), which is often based on internationally adopted rules and practices. In this context, a good practice is usually the adoption of stricter rules and more demanding parameters to avoid potential problems. A case that exemplifies the use and self-regulation of the technology is that of the Brazilian Judiciary Branch. A survey carried out by the Center for Innovation, Administration and Research of the Judiciary Branch (CIAPJ) of the Fundação Getulio Vargas (FGV) indicates that half of the courts in the country have an AI project under development or even implemented39, which is done seeking, among other things, greater efficiency, productivity and procedural speed. Thus, there are tools designed, for example, to categorize and search for case law, transcribe voice to text, identify whether a lawsuit is linked to any precedent, and semi-automatically generate procedural instruments. Aware of this movement, the National Council of Justice (CNJ) issued Resolution No. 332/2020, which provides for ethics, transparency and governance in the production and use of Artificial Intelligence in the Judiciary Branch, and Ordinance No. 271/2020, which regulates the use of Artificial Intelligence within the scope of the Judiciary Branch. Besides the specific regulation of AI – non-existent in Brazil –, there are some other laws applicable, directly and indirectly, to those who use the technology, with a focus on the LGPD and Internet Civil Framework. Because of their importance to AI, we will address these laws in a separate item. 3.2. The International scenario Internationally, the regulatory debate on Artificial Intelligence is in a more advanced stage. It is possible to identify the issuance of more robust national plans as well as specific laws on AI, which address issues such as accountability and robotics. Even so, regulation is fragmented and there are also countries at a less advanced stage, for which it is necessary to outline more clearly the implications of AI, the limits and possibilities of action in society and in the economy, among other factors. In any case, the analysis of existing standards allows us to identify certain constants, such as the importance given to the principles that guide the use of an ethical, responsible and reliable Artificial Intelligence; the focus on humans and on protecting the planet; the need for algorithms to be explainable and transparent; technical and security robustness; human autonomy; and diversity, justice and equality. The debate on accountability in the field of AI has also made advances. Recently, in 2021, Europe released a proposal for a general regulation on AI with a risk-based approach. This is the Artificial Intelligence Act (AI Act), which sets out specific rules for the various systems and applications of the technology. The proposal is the outcome of an extensive process of debate and publication of guidelines by the European Commission. Previously, in April 2019, the Commission’s Independent High-Level Expert Group on Artificial Intelligence published the “Ethical Guidelines for Reliable Artificial Intelligence”. The document recognizes the potential of AI, but also pays attention to the risks, seeking to address how to deal with certain problems. Emphasizing that a reliable AI must be legal, ethical and robust, the document addresses issues such as accountability, human autonomy and systems oversight, as well as technical robustness. It also provides principles similar to those already covered in this Guide. The following year, the Commission published the White Paper “On Artificial Intelligence – A European approach to excellence and trust”, giving continuance to the guidelines to be followed and pointing out future regulatory actions. Other measures, such as public consultations, were adopted until reaching the aforementioned regulation proposal of 2021. In the United States, the Algorithmic Accountability Act, of 2019, defines which systems that involve personal data or make automated decisions are considered to be of high risk, presenting requisites to be followed in these cases. The Commercial Facial Recognition Privacy Act, also of 2019, prohibits the processing of facial recognition data, except in the event that the organization presents documentation on the capabilities and limitations of its technology and there is express affirmative consent from the end user preceded by notification about the reasonable uses for this type of data. In turn, the Self Drive Act, of 2017, establishes rules for testing and implementing automated cars, in addition to other provisions on the subject. Local governments have also acted to regulate AI. The city of New York, for example, has approved the New York City Automated Decision Systems Task Force – ADS Task Force, aimed at government agencies that use algorithms in decision-making processes. In general, the purpose is to assess whether the algorithms are consistent with the purposes of making the city more just and equitable. The State of Washington is discussing a bill aimed at eliminating biases in automated decision-making processes. In the context of adopting national plans, China should be highlighted, which has an ambitious AI strategic development plan. Seeking to become the world’s leading country in implementation of AI technology by 2030, the New Generation Artificial Intelligence Plan (AIDP) was launched in 2017 and is focused on the areas of international competition, economic growth and social governance40. Among other countries that also have plans, we can mention Australia, with the Artificial Intelligence Ethics Framework, of 2019, and Germany, with The German Strategy for Artificial Intelligence, of 2018. Artificial Intelligence is closely connected to other technologies, besides being based on large-volume data usage. One of the initial steps in programming and defining how an AI tool works is to determine what data it will rely on to work and generate the expected results. This is because AI uses a large amount of data – personal and even sensitive data41, oftentimes – and generates new data. This is not a simple task, but it is essential for the proper performance of the technology and, accordingly, for a company’s own performance, since the lack of definition or disorganization of such data can produce negative outcomes, either by delaying processes or generating undesired legal effects, or even increasing the risks triggered by the systems themselves. Therefore, the use of AI requires compliance with other legal rules, such as those related to data protection and cybersecurity. Such compliance is paramount and is related to the idea of resilience or robustness of the AI, that is, companies must have “technical robustness and compliance of their AI and its agility in all platforms and resistance against malicious agents”42. In addition, due to the creative, copyright and also industrial nature of AI, the discussion about Intellectual Property in this field becomes relevant. There are questions to which the IP regulatory framework already provides clear answers. Others, however, are still in the field of debate. In this regard, the European Parliament, for example, published a resolution in October 2020 to regulate the relationship between IP and AI. Thus, we shall analyze here the main rules on data protection, cybersecurity and Intellectual Property that must be followed by those who apply or intend to apply Artificial Intelligence technologies. We emphasize that, beyond the cold observance of the law, companies tend to benefit even more when a culture of respect for data and cybersecurity is created. In other words, all the chains of a company must be guided by a common logic of respect and attention to data protection standards and principles, such as collecting only what is necessary for the proposed purposes, adopting appropriate storage techniques, respecting security measures and the like. This point will be further explored in item 5 of this Guide. 4.1. Brief analysis of the regulatory scenario Within the context of protection of personal data and the internet, two laws gain relevance. First, the General Law for the Protection of Personal Data (LGPD) (Law No. 13.709/2018)43, which regulates the processing of personal data, establishing principles to be followed, rights of data subjects, rules for processing44 (such as for collection, use and storage), responsibility of the actors involved in this process, sanctions, and even encourages the formulation of good practices and governance on the subject. Thus, the Law specifies the ways to protect the fundamental rights of freedom and privacy and the free development of the individual’s personality in the context of the use of personal data. Second, there is the Internet Civil Framework (MCI) (Law No. 12.965/2014), which is aimed at the use of the internet, setting out principles, users’ rights, aspects of registration and personal data, liability for damages, among other topics. In addition, there are other specific rules to be observed, depending on the case and area of activity of each company, as already mentioned. In the international scenario, we highlight the General Data Protection Regulation (EU GDPR 2016/679), which regulates the processing of personal data in the context of the European Union. Considering that the LGPD was drew strong inspiration from this regulation, the laws have great similarities. The rules of the GDPR must also be observed by those who, even in Brazil, process the personal data of data subjects from the European Union. Other international laws may also apply to Brazilian companies, depending on the origin of the data, the residence and citizenship of the data subjects and the commercial relationships established. This is the case, for example, of the California Consumer Privacy Rights Act, which will become effective as of July 2023, and of the Stop Hacks and Improve Electronic Data Security Act (New York’s SHIELD Act). It is also worth mentioning the approval, in China, of the Personal Information Protection Law (PIPL), which bears great similarities with the GDPR and the LGPD. 4.2. Personal data protection The use of AI applications, especially in light of the benefits they can generate for a company, can cause a desire for data collection in increasing amounts, which tends to be beneficial for machine learning and deep learning techniques, for example. However, careless collection can have negative consequences for the company, including the application of sanctions. Therefore, it is essential, in relation to any data collection, to pay attention to the rules on data protection set out in the LGPD. The Law provides for the limitation of the processing to the minimum necessary for the accomplishment of its purposes, with the scope of pertinent data, proportional and not excessive in relation to the purposes of the data processing. To this is added the idea that processing, including collection and use of the data, must comply with the legal rules, such as the requirement of a specific purpose duly informed to the data subject and that such processing must take place in a manner appropriate to the proposed purposes, among other rules that are established by the LGPD. It should also be noted that data cannot be stored indefinitely and without a purpose for its storage. There are specific rules determining the adequacy of the storage, the possibility of accessing the data by the data subject and, above all, a specific period for this storage. After the intended use, the data must, as a rule, be deleted. An alternative to this is irreversible anonymization, which removes the personal character of the data. Similarly to when we refer to the adoption of ethics by design, the perspective of privacy by design is also strongly recommended, in regard to the protection of data. In general terms, it refers to observing and respecting privacy at all stages of the system, from its inception. There are seven principles guiding the use of this technique, summarized below: The LGPD also affirmed the right to explanation for the field of personal data protection. This right applies to those who use Artificial Intelligence applications that use personal data. The Law provides that, “[the] data subject has the right to request the review of decisions taken solely on the basis of automated processing of personal data that affect their interests, including decisions aimed to define their personal, professional, consumer and credit profile or aspects of their personality.” Although the need for the review to be carried out by a human person has been removed from the Law, the doctrine has advocated a review under these terms46. Human supervision is even an aspect that is recurrently highlighted as necessary for an ethically and legally responsible use of AI. This provision of the LGPD, which is similar to what is stated in Article 22 of the GDPR, also reinforces the need to keep records of processes, data usage, AI activities and algorithms in general. 4.3. Cybersecurity With the concept of cybersecurity, the aim is to adopt technical and administrative measures that ensure the security and integrity of systems (software) and equipment (hardware), networks and digital infrastructure, as well as data protection47 in the cyberspace, safe storage and technical robustness. In brief, the aim is to have an adequate and safe environment for the processing of personal data and for the operation of AI systems, free from leaks and undue access, with the prevention of incidents such as accidental data destruction, programming errors, among others. In accordance with information security rules, it is necessary to ensure data confidentiality, integrity and availability. For this purpose, it is necessary to anticipate possible incidents, such as hacker invasion. This must be an ongoing concern accompanied by constant updating of security standards, which is reinforced by the fact that even techniques considered highly secure are, at some point, contested, as is the case with biometrics48. In this respect, there are AI tools that can be used to detect threats and prevent their materialization, seeking solutions capable of overcoming a particular problem. AI solutions can be used, for example, to verify the identity of who is accessing a particular account or system and to check for unusual and/or inappropriate usage and access patterns. Appropriate hardware and software licenses can be expensive, but there are also open-source options available. Reinforcing the concern related to the subject and the need for concrete actions, the National Cyber Security Strategy49 was approved in Brazil, in 2020, through Decree No. 10,222/2020, guiding the actions to be adopted by the Federal Government until 2023. 4.4. Intellectual Property With the advances and the increase in the use of Artificial Intelligence, a subject that has gained prominence is its connection with intellectual property (IP). In this relationship, there are points of contact and tension, which are intensified by the strong industrial and/or artistic character of AI. On the one hand, IP provides legal tools to ensure protection for intellectual creations, such as for patenting technologies and for copyright. On the other hand, there are difficulties arising from the very functioning of AI: it is not always possible to clearly determine who is the creator of an AI technology, especially the more complex ones, which involve numerous codes and algorithms. Traceability of intellectual property rights becomes a difficult task in these scenarios. In the Brazilian regulatory context, the following laws gain relevance in the field of the connection between artificial intelligence and IP: Law No. 9,610/1998, known as the Copyright Law; Law No. 10,695/2003, which deals with violations of copyright; Law No. 9,609/1998, known as the Software Law, which deals with the protection of software intellectual property; Law No. 9,279/1996, referred to as the Industrial Property Law; and Law No. 11,484/2007, which establishes protective provisions for the topography of integrated circuits (chips). In the international context, it is worth highlighting the role of the European Parliament50, which, in October 2020, published a resolution on “intellectual property rights related to the development of technologies related to artificial intelligence” (P9\_TA(2020)0277). With technological development, new discussions have emerged, which are also accompanied by reflections on the extent to which IP laws will need to be changed. This is the case, for example, with the debate on attributing authorship to creations made by an AI system. Under the current Brazilian Copyright Law, an author is only the “individual who creates a literary, artistic or scientific work” (Article 11, caput, of Law no. 9.610/1998). Thus, in the current legislation there is no possibility of attributing authorship to the machine. However, going beyond the current regulation, there is a reflection on the theme in the academic sphere51, which may, in the future, lead to changes in the law and new regulations as the technology advances. We already have concrete examples of this issue. In 2016, from the analysis and identification of patterns in paintings by the painter Rembrandt, an algorithm created a new painting that became known as The Next Rembrandt52. Another example is the science fiction short film ‘Sunspring’, whose screenplay was written by AI system53 from the analysis of numerous film scripts of the same category. This discussion delves into machine learning and deep learning systems which, after being taught, continue to learn on their own new ways to find the solution to a problem and to give the answers sought. The more complex the technology, as in the case of deep learning and neural networks, the greater its distance from its creator and the more difficult it is to understand how the machine reached a certain result, making it difficult to assign the referred rights. The level of human interaction with the system is also often identified as an important factor in this equation. Finally, AI has also contributed to the identification and processing of intellectual property rights more quickly than human beings, reducing costs and optimizing time. This is the case, for example, of two YouTube systems: the Copyright Match Tool, which identifies matches or possible matches of videos on the platform, to be analyzed by those who request removal by copyright; and the ContentID, which analyzes the videos posted on the platform and identifies if there is use of any content of a copyright owner, in which case the owner will have certain options, including blocking the viewing of the video. As observed throughout the previous chapters, Artificial Intelligence is already a reality present in a large number of organizations as well as in people’s daily lives. Many companies already use AI in their procedures and products or are exploring its potential. The absence of specific regulation on the technology in Brazil is not enough reason to prevent its use. Based on constitutional principles, other laws and especially the framework of principles internationally widespread on AI, the regulatory debates carried out and operation of companies already advanced in this process, it is possible to infer certain concrete measures to be taken for an ethical, responsible, and reliable implementation of AI. Thus, we shall present, in this item, recommendations and good practices to be observed along this path. These are measures that are related to ethical principles and whose consideration is necessary in all stages of a company’s digital transformation, from the beginning of planning AI incorporation to its results and uses in the company’s products. 5.1. A culture of data and ethical, responsible, and reliable performance of operationsperformance of operations First, it is essential to develop a culture focused on Artificial Intelligence, covering issues such as data protection and cybersecurity. We do not ignore that a cultural change in the company is not a simple task. However, organizations have in their favor the fact that the digital transformation has been taking place for some years and people in general are already able to embrace and integrate technology into their daily lives, although in simpler ways. Therefore, this change in the internal culture comes in the midst of the flow of external transformations and amounts to adapting our way of living, working, generating products, among other things. For Patrícia Prado, there are three fundamental points to be observed in this cultural change54. First, the change must come from the company’s leaders, who need to “understand what this culture change means and participate in it”55. In other words, it is necessary that the concern about data and cybersecurity and the cultural change are noticeable in the actions, plans and statements of the company’s directors that will gradually transmit and strengthen this culture to the other employees. Second, Prado highlights the need to “choose metrics based on key business objectives”. Accordingly, the company’s objectives must be well defined, as well as the operating strategy to achieve them and the measures for their constant evaluation. Finally, the author points out that it is necessary to build a “reliable and transparent database”, which includes joint action between the business sectors and the technology sector. We have addressed this point above, by mentioning the need to define and organize the data already during preparation of the AI. Here, we point out the need for such care to be observed throughout the use of AI, even impacting the form of relationship between members of the company. This culture encompasses not only aspects directly linked to data, but also requires respect for ethical principles on Artificial Intelligence. These principles, mentioned in item 2, must be respected at all stages of the AI. Thus, they need to guide the process of planning objectives and strategies, so that issues such as damage prevention are already considered in this project. As we will see, the principles are not as abstract as they might appear at first reading. In fact, they relate directly to good practices that will be addressed here, and which seek to ensure factors such as transparency, accountability, responsibility, and assurance of the review of decisions. 5.2. Internal mapping and strategy definition In order to develop a culture in the sense mentioned in the previous item and to implement AI projects, it is essential that an internal mapping is prepared. Before applying changes and including new technologies, it is essential to analyze what the intended objectives are, which strategies will be adopted to achieve them, what tools and infrastructure are available, what level of qualification and training of the team is already part of the company, and, mainly, what problems are faced throughout the processes. AI solutions must be well targeted to specific issues and come with cross-sector support. Otherwise, they will not deliver the expected benefits. In other words, it is necessary to identify where technology can be used to improve the company’s processes, which area requires changes and can benefit most from the transformation, especially in a scenario where there are limited resources. This also involves analysis of already existing results and sincere conversation with all the employees, who are involved in the dayto-day activities and are aware of the details of the company, and who will thus provide more accurate insights, pointing out needs for improvement and bottlenecks. From there, the strategy can be designed, which will certainly involve the implementation of some changes, such as hiring and/or training of personnel, enhancing computer infrastructure, purchasing software licenses and purchasing equipment. In general, there will be a redefinition of the business model, which will be based, even partially, on AI. The products will be distinguished and further improved. One thing to be considered while still in strategic planning is the need to dedicate time to the execution of pilot projects, in order to analyze whether the technology is well adapted, whether it is generating the expected results and which aspects should be improved before the actual execution. It is a project to be thought out and applied with caution, mapping and with the mitigation of risks in mind. Finally, we emphasize that it is desirable that this internal mapping be redone with some regularity, in order to identify flaws and gaps. 5.3. Chart of Professionals /inclusiveness In the sequence of the mapping and definition of the company’s strategy, it will be necessary to focus on the adequate body of professionals. A team responsible for AI must be organized in the company, in charge of its planning, monitoring and execution. This team must involve, among others, engineers, data scientists, product manager, marketing analyst, person in charge of personal data processing (Data Protection Officer – DPO), and a legal team with interdisciplinary knowledge. An available alternative is the contracting of other companies to perform one, some or all of the steps of implementing and executing projects, which will not require a full AI team in the company. This can be useful for small companies, which cannot yet afford this type of investment; for those that want to take it slow and test AI solutions before incurring huge financial expenses, hiring personnel and changing their infrastructure; or also for large companies that, despite the high number of employees, might not have expertise in one or more areas essential for AI. For all companies, regardless of their size, hiring an external professional responsible for the organization’s compliance is a positive step, as the person will be someone with a posture that is not biased by the company’s procedures and will have greater capacity and freedom to point out deficits and recommend improvements. A company tends to benefit from a body of professionals with diverse training and backgrounds56, which also includes aspects of diversity, such as race and gender. This will allow everyone to contribute from different perspectives, which will prevent risks – as a wider array of people will be analyzing the possible consequences of a project – and will increase the potential for using the technology. Thus, although the formation of this diverse and specific group may demand some investment, it will prove to be a great competitive advantage. The diversity will also demonstrate its benefits upon formulation and setting of algorithms, allowing the identification of biases from the perspective of gender, race, age, nationality, among others. Thus, the company takes an important step to ensure respect for the principle of justice. 5.4. Personnel training Even with the hiring of specialized personnel, it is also important to invest in the qualification and training of current employees, so that everyone is integrated with the new technologies used in the company. It will be necessary to present and teach how to use the system, provide training on ethical and legal aspects, among others. 5.5. Creation of comprehensive privacy and data policy The creation of a privacy policy aimed at the user that makes clear all forms of processing of personal data is already a requirement of the LGPD. In the context of Artificial Intelligence, this will continue to be a duty of companies, but such documents will have to be improved in order to also make clear the procedures involving technology. This will meet a requirement for transparency and will reinforce reliability, in addition to serving to standardize the company’s behavior. Thus, in addition to listing all the processing of personal data carried out by the organization in its wide variety of operating contexts, it will be necessary to explain the uses of AI and the way in which the data relate to it. The internal mapping and definition of objectives and strategies will be fundamental at this time, as they will serve as a complementary guide to the policy. The document should contain a presentation of possible risks and their levels, followed by actions to mitigate them. Issues such as mechanisms for systems oversight, planning in cases of incidents and methods for compliance with ethical principles and legal rules should also be included. The document must be easily accessible by the data subjects/user of the technology and present simple and easy-tounderstand language, in addition to allowing the data subjects to effectively exercise their rights related to data protection. 5.6. Impact analysis and risk assessment As already mentioned, the use of AI applications requires constant attention to identify possible risks and act in order to mitigate them. It is necessary to always adopt a preventive stance. There are different parameters for identifying risk levels and the requirements for each. Allianz, for example, identifies three levels of risk in AI applications and in the use of personal data, categorized according to the difficulties in overcoming them and their probability of causing harm57 : 1) Low risk: there may be some risks and inconveniences, but overcoming them tends to be simple and the occurrence of errors is quite low; 2) Medium risk: even though the probability of incidence is low, there are significant chances of inconveniences, whose overcoming brings some difficulties; 3) High risk: the inconveniences and consequences are more serious, with major difficulty to overcome them, and they might even be irreversible. The probability of damage is high. The risks and impacts of AI vary both by the technology itself and context. Therefore, determining the level of risk and human involvement must be done on a case-by- case basis. For this, Allianz58 recommends considering the following aspects: Data Category The use of sensitive data automatically leads to a medium level of risk, a trend that is often followed by data from social networks as well. For example, because of the amount of sensitive data and the impact of decisions, a health insurance company is classified as high risk. Type of client The use of personal data from vulnerable groups also carries a medium risk; Impact on the client Legal consequences, impacts of financial aspects and long-term decisions must be taken into account. Thus, an automated decision generates an average risk, which can be reduced by the possibility of explaining, challenging and even reviewing the decision. Financial issues, when problematic, increase risk, as do irreversible long-term decisions. Field of application Issues such as advertising without profiling and automating internal processes are often low risk, but it is possible that a combination of several low risk applications creates a high risk scenario. Mitigation of these risks involves aspects already mentioned, such as applying technologies that have an adequate level of development and maturity; ensuring that technical and cybersecurity requirements are respected and systems are updated; and anticipating and preventing the occurrence of biases and discrimination, which involves comprehensive training on the system and feeding it with varied data As stated, there are other parameters to identify, categorize and regulate AI applications according to the actual risks. The proposed regulation of Artificial Intelligence in the European Union - the AI Act mentioned in item 3.2. of this manual - establishes a risk-based approach, but without creating unnecessary restrictions. The idea of forecasts, in general, is to deal with situations where there is justified concern or that such concern can be reasonably anticipated in the near future, so that the AI is reliable, safe, respects legal rules and generates benefits for European citizens.59 Therefore, the proposal seeks to: deal with the specific risks of AI applications; define which systems are high risk and which requisites must be met in these cases; propose the conducting of a compliance assessment prior to putting a high-risk AI into service or on the market; and also to propose a governance structure at the European and national level. In this way, the proposal presents four different risk levels, ranging from low to unacceptable risk. Each one demands the observance of specific rules, and requirements are expressly provided for in the proposal. There are even some exceptions to the general rules of risk classification and restriction and/ or prohibition of use. Presented below is the outline60 for each of the risk levels: Unacceptable risk Particularly harmful AI applications and prohibited for violating values of the European Union, such as systems for subliminal manipulation of individuals and systems for real time distance biometric identification at public sites for security purposes. High risk Systems that pose a high risk to health, safety and fundamental rights of people. They are subject to predictable mandatory requisites to ensure safety and respect of fundamental rights throughout the system lifecycle; Limited risk Systems subject to minimal transparency obligations, as in the case of chatbots; Low risk Applications with free use in the European market; 5.7. Algorithm auditing In general, algorithm auditing aims to “evaluate the consistency of the models in relation to the principles and standards in force, focusing on the review of source codes and the impacts of the ‘outputs’ of the algorithms (predictions indicated by the models)”61. In other words, the auditing of algorithms seeks to analyze compliance with legal rules, such as data protection and ethical standards, added to the adequacy of cybersecurity techniques and requirements. The focus is on the practical aspect, that is, if and how the rules and principles are applied in the systems and processes. In addition, the algorithm itself is also analyzed, how it was programmed and which code was used62, in addition to the results obtained, in order to ensure that they are not discriminatory. In short, this is an important governance and compliance mechanism, aimed at analyzing AI behavior. With this broad objective in mind, some examples of specific aspects to be verified and some audit tasks are: “to support the decision-making, visualize and monitor the results; inform users of why a decision was made and how to challenge it; alleviate human suffering by anticipating and mitigating damage; allocate responsibilities; and balance conflicts of interest”63. The audit can be carried out by a government agency, by an outsourced professional hired for this function, or it can be a task specifically assigned in multilateral organizations64. It is important that it be carried out independently from the other tasks of the company. Note, however, that auditing is not and should not be seen as the single and most important mechanism for ethical and legal compliance. It is a fundamental mechanism that is strongly related to the idea of transparency, but which should be one among several measures and good practices adopted by the company to ensure ethical, responsible and reliable use of AI. There are even some issues and obstacles to be observed in an audit, such as the difficulty of interpreting an algorithm, the different behavior of the algorithm in different contexts65 and its mutation in contexts of machine learning and deep learning. Thus, for ethics-based auditing to be viable and effective, Jacob Mokander and Luciano Floridi point out that it must: (i) be a continuous process; (ii) be Good Practices in Artificial Intelligence - A Guideline 50 part of the sociotechnical system as a whole, and not something isolated; (iii) be seen as a dialectical process, and not a static and preconceived process, ensuring that the appropriate questions and expected answers are given according to that context; (iv) be aligned with organizational policies and incentives; and, reinforcing the importance of ethics by design (v) “interpretability and robustness must be incorporated into systems from the beginning. Ethics-based auditing supports this purpose by providing active feedback to the continuous process of (re)design”66. In the Brazilian data protection scenario, the provisions of the LGPD, focusing on the principle of transparency, the provisions on accountability and the right to review automated decisions, all reinforce the idea of auditing. There is an express provision attributing competence to the Brazilian National Data Protection Authority (ANPD) to “perform an audit to verify discriminatory aspects in the automated processing of personal data” (Article 20, § 2) in the event that the controller does not provide “clear and adequate information regarding the criteria and procedures used for the automated decision” (Article 20, § 1) and generic provision in Article 55-J, XVI. 5.8. Report preparation Finally, it is recommended that reports are prepared detailing how the systems were developed and applied, which processes were implemented and what results were obtained. The preparation and maintenance of up-to-date documents and reports is beneficial for any potential audit and for meeting the accountability requirements. This will also provide clearer control and analysis of processes and systems. Thus, in line with the internal mapping, continuous control of systems and “retrospective impact assessments, carried out in the form of self-control and/or third-party control”67, contribute to maintaining security and respect for ethical principles and legal rules. As observed by Wolfgang Hoffmann-Riem: In this item, we briefly mention some successful examples of principled approaches and concrete uses of the technology that forms the scope of this manual. The objective is to point out, on the one hand, that there is room for success with the use of AI, while on the other, to ascertain what these concrete experiences can teach us. First of all, we return to an idea already mentioned briefly: that international organizations have also played an important role in this context. The OECD, for example, brings a principled approach to the technology with the aim of promoting an AI that is “innovative and reliable and respectful of human rights and democratic values”. For the organization, responsible use of reliable AI involves observing 5 complementary principles, which can be summarized in the following ideas69: i) be beneficial to people and the planet, stimulating sustainable development and well-being; ii) respect for the Rule of Law and adoption of safeguards to guarantee a fair and equitable society; iii) transparency and explanation; iv) robustness and security; v) accountability. These principles have been incorporated by an increasing number of countries and have served as the basis for the elaboration of principled approaches by countries and organizations, such as the G20. This shows us the importance of a unified perspective of principles and the potential of its existence. A concrete example of positive application was observed through Amazon’s Alexa. The famous virtual assistant was the target of concern from parents and associations dedicated to the rights of children who noticed a cold and protocol-based communication in minors. Through a politeness feature strategy, the company programmed the virtual assistant to encourage children to say things like “please” and “thank you”70. This case illustrates the attention to the principle of beneficence, focusing the use of AI to be aimed at the welfare and benefits to humanity, in addition to exemplifying the possibility of improvement and revision of technology as it is used. It also demonstrates how a use of ethics by design can work, as these aspects had to be considered at the time of designing the technology. Finally, it is worth mentioning briefly that there are also negative examples of the use of AI. Image recognition with discriminatory results; the unexpected behavior of chatbots, who end up learning prejudiced speech; inappropriate content recommendations; and the generation of deepfakes and the influence of this category of information on AI systems are some of the negative results to which companies should already pay attention to adopt preventive action now. Even without specific comprehensive regulation on AI, ethical principles, international regulations and even national laws on related topics indicate paths that must be followed by those who already wish to adopt the technology. With its potential already quite clear, Artificial Intelligence will bring many benefits to organizations, and those that start preparing now will have a great competitive advantage over other companies, in addition to already taking action to avoid risks. Bearing this in mind, we have prepared below, in a simplified way, the main steps that should be taken proactively by companies that have encountered Artificial Intelligence, are considering integrating it into their processes and products and do not yet know which path to follow. 1. Develop a data culture and pay attention to the ethical principles of AI at all stages of its application, from planning to its actual use and analysis of results. As mentioned, several principles have emerged to delimit and guide the possibilities for using AI. An analysis of these principles indicates a consensus of ideas to make Artificial Intelligence accountable, transparent and reliable. These ideas are translated into the principles summarized briefly in the table below: Beneficence AI must be used for the benefit of Mankind, focusing on the well-being of people, respecting human dignity and paying attention to the planet’s sustainability. Non-maleficence Use of AI should not cause harm, and it is necessary to anticipate and prevent risks and adopt safety techniques. Autonomy AI may not weaken or eliminate human authority. Users must be assured the autonomy. AI should promote justice, exclude any prejudice, discrimination and biases and should promote aspects such as solidarity, equity and diversity. Justice AI requires that its use be inteligible (user should be able to undestand how the system works) and there must be accountability (responsibility 2. Map the company’s personnel, resources and rules to identify gaps and areas where investment should be increased and processing should be enhanced. It is recommended to hire specialized and diverse personnel, in addition to training the entire workforce of the company; 3. Create policies for the use of AI, data protection, security and other aspects, in order to make clear the general technical, behavioral and security standards to be observed by the company as a whole. It may be necessary to redefine or adapt the planning and business model; 4. Create an AI governance in the company to be observed at all stages involving the technology and its projects, such as strategy, implementation and monitoring. It may be appropriate to create “separate governance committees and councils to deal with the exclusive risks and complexities associated with AI and data”71; 5. Encourage studies and projects aimed at delivering AI solutions through the creation of a framework for this purpose, which should be guided by clear guidelines be supplied with appropriate tools and investment72; 6. Invest in risk analysis, creating a responsible structure that is capable of identifying risks in advance and acting to mitigate and avoid them, which may involve the very use of algorithms to identify and manage risks. This includes a joint review with cybersecurity teams and requires attention to aspects of ethical integrity and technical robustness; 7. Prepare and maintain documents and reports on the creation of algorithms, their application and their results. This favors continuous analyses, allows for the modification of systems that produce unwanted results, helps to prevent risks and proves to be useful in carrying out a potential audit.

158. [AI, Data Protection & Privacy 2024 legislation](https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2024/brazil)

[Lopes Pinto, Nagasse Advogados](https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2024/brazil) is based in São Paulo. The firm provides expertise across many areas, including corporate and business law, tax and planning, data protection (LGPD, GDPR and PIPL), contracts, regulation, digital assets, blockchain, transportation, logistics, labour, infrastructure, agribusiness, banking and finance, bioscience, civil law, corporate governance, compliance, tech law, and legal risks. The team of highly skilled professionals possesses in-depth experience of national and multinational companies and law firms, and the modus operandi of organisations and businesses. Lopes Pinto, Nagasse Advogados prides itself on being a highly ethical firm, focused on achieving results and providing excellent service to its clients. Since 2006, it has been recognised as one of the most highly regarded law firms by Época, a Brazilian news and analysis magazine.

Close All

1. Basic National Regime

 1.1 Laws

The Development of Data Protection Legislation in Brazil

In Brazil, data protection regulation – especially protection of personal data – stems from the Constitution (Article 5, X): “intimacy, private life, honour, and image of people are inviolable, ensuring the right to compensation for material or moral damage resulting from their violation”.

The Consumer Protection Code (Law 8,078/93) also has rules on “personal information”, and introduced, for the first time, a standard that allows consumers to have access to the data that a company holds about them and to request its update or correction. These concepts were expanded by Decree 7,962/13, which now talks about “data security”, an idea close to another concept, that of “personal data as part of an individual’s assets”.

In 2013, the Civil Rights Framework for the Internet was approved (Law 12,965/14). Even though it was aimed at activities on the internet, it introduced relevant concepts, such as “net neutrality” and “active protection of personal data”, into the wider legal/regulatory landscape in Brazil.

In 2018, with Law 13,709, the General Data Protection Law (LGPD), introduced rules designed to regulate, protect, and discipline the treatment and security of personal data in Brazil. Based almost entirely on the GDPR of the European Union, the LGPD only entered into force in September 2020, except for its penalties.

In 2022, the protection of personal data was explicitly included in the Federal Constitution as a fundamental right (Article 5, LXXIX).

With the advancement of AI, Brazil decided to try to regulate the matter. To this end, Bill 2,388/23 emerged, which, in line with global trends, is based on the most widely accepted principles in this area:

recommendations and ethical principles for creating standards of conduct;

rules on governance and compliance;

a certain degree of normative liberality in the practice of AI; and

the establishment of rights and obligations with the aim of mitigating risks and ensuring reliable use of AI systems.

 1.2 Regulators

Principal and Derivative (Sector-Specific) Regulators

The Brazilian regulatory model is largely based on the GDPR, and adopts a similar “vertically centralised” regulatory system. Regulation is part of a “hard core”, represented by the Constitution, which runs along the central axis (legal framework) and ends in the branches (regulation and rules).

This model admits some radicality, in which the regulation assumes a “horizontal” profile, reaching not only those that directly engage with the processing of personal data, but the entities that exercise some regulation over data processors.

Thus, there are two classes of regulators: the principal regulators, which receive prerogatives from the primary legislation (Constitution and LGPD), and the derivative regulators, whose regulatory power stems from the fact that the activities of a given data processor are under their regulation.

The main regulator is the Autoridade Nacional de Proteção de Dados (ANPD), as provided for in the LGPD and approved by Decree 10,474/20. Recently, the ANPD has gained the status of “agency” and has begun to make up part of the structure of the Ministry of Justice. Among derived regulators there are some entities, such as the Banco Central do Brasil (Law 4,595/64), the Agência Nacional de Transportes Terrestres (ANTT) (Law 10,233/01) and the Comissão de Valores Mobiliários (CVM) (Law 6,385/76).

Although the ANPD argues that the punitive measures referred to in the LGPD are of exclusive application by the main regulator, this is not exactly true, as there are penalties substantially like those of the LGPD that can be imposed by secondary regulators. Thus, the sanctions applicable by the ANPD can perfectly coexist with the sanctions imposed by a secondary regulator, especially if the facts assessed by both regulators are related to the protection of personal data.

AI

As for AI, the matter gets complicated. While the ANPD wants to take over the regulation of AI, due to the proximity of the subjects within its competence (personal data) to the topics related to AI systems, other voices say that regulation should take place in the form of a “committee”, composed of other government bodies. Bill 2,388 is silent on the topic, limiting itself to referring to a “competent authority”.

In the EU, the AI Law seems to indicate a very strong desire for the bloc to become a “global regulator” on AI issues, given the repercussions of its regulations on other countries, including Brazil. Furthermore, the AI Act shows a well-defined focus on technology risks, the so-called “own risks”, especially its effects on disinformation, innovation, jobs and the interests of governments and States.

The topic of “deepfakes” is one of these own risks. People are misled by fraudulent video and audio content, created with the help of AI. Precisely for this reason, in Brazil, Bill 5,241/23 is being processed, which establishes the use of deepfake audiovisual content as a crime.

 1.3 Administration and Enforcement Process

Brazilian legislation on personal data establishes a process for sanctions and a means to challenge such sanctions. This begins with the administrative process carried out by the ANPD, which verifies an organisation’s adherence to the LGPD.

The process may be monitoring, guidance, prevention or repression. If the supervised agent does not adjust its procedures, the regulator may apply the sanctions. Even in this case, regulatory authorities and agents may sign a conduct adjustment, to be completed within a certain period.

In the event of a penalty, the regulator must comply with the following criteria:

compliance with the general interest;

adequacy between means and purposes, formalities essential to the guarantee of rights, simple forms;

respect for the rights of interested parties;

official operation of the administrative process (without prejudice to the actions of the interested parties); and

legal interpretation to ensure the fulfilment of the public purpose.

The regulated organisation has means of defence; however, ANPD Resolution 1/20 begins by declaring (Article 38) that there is no way to appeal the decision of the regulator that opened the sanctioning process, which calls into question the right to appeal. First, the Constitution says that no law can exclude from judicial assessment an injury or threat to the law (Article 5, XXXV); second, the Constitution affirms (Article 5, LV) the principle of broad defence; and third, the Federal Administrative Procedure Law (Article 2, paragraph 1, X), applicable to proceedings before the regulatory authorities, determines that it is the right of the interested party to appeal as it deems necessary.

According to the infraction notice, the regulated agent has ten working days to defend itself, including with evidence and other elements; then, the regulated agent has ten more working days, before the instruction report, to respond to the evidence and other elements collected; finally, the agent will be called to comply with the decision, or to make a final appeal, within ten working days, addressed to the Board of Directors of the ANDP.

If the regulated agent does not agree with the decision of the council, it may appeal to the judiciary. Since the ANPD is now part of the structure of the Ministry of Justice, discussion has gained momentum over whether, in the case of a final decision of the ANPD, and before taking the matter to the judiciary, the penalised agent could submit an improper hierarchical appeal – the legislation seems to allow this exit, but only time will tell.

AI

As there is still no legal framework for AI in Brazil, it is not possible to say that the country has a system of sanctions and resources focused on AI issues. This does not mean, however, that there is an absolute vacuum. If an AI issue has to do with personal data, it is always possible to submit it to the ANPD. If the issue is related to the financial market, it is possible to take it to the CVM or Central Bank for examination.

 1.4 Multilateral and Subnational Issues

The Brazilian national regime for the protection and guarantee of personal data is quite recent (2018), even though discussions on the subject began more than a decade ago.

Brazilian legislation has a low level of interaction with the legislation of members of the Asia-Pacific Economic Cooperation (APEC), but many issues have been discussed bilaterally. One of them is the protection of personal data in cross-border trade; for example, considering the “inherent risks” of unregulated transfers, parity of legal standards, alignment between commercial partners and alternative means of conflict resolution.

The interaction between Brazil and the EU is far greater. Of particular note is a difference in the interpretation of jurisdiction over data processing. For Brazil, personal data processing is subject to the LGPD if, as a fundamental concept, this processing occurs within the national territory. Under the GDPR, however, the processing (or processing) may still fall under EU regulation even if carried out by a controller outside the EU, if it is sufficiently linked to the activities of an establishment in an EU country.

Brazil has expressed interest in joining the OECD, but to do so it would have to make progress in personal data protection and the regulation of fair and legal data processing acts. The case of the European Directive on Electronic Privacy is emblematic: the EU is already discussing escalating the issue to more complex legislation, but Brazil does not even have fundamental guidelines on the subject.

 1.5 Major NGOs and Self-Regulatory Organisations

Data protection and security in Brazil is still a very recent issue, and therefore there is not a significant number of independent bodies dedicated to maintaining data protection and security standards, especially personal data (eg, self-regulatory organisations (SROs) and others).

In recent months, some initiatives have been observed in this area. For example: the case of the self-regulation agreement between the CVM and ANBIMA (an association that brings together financial and capital market entities). Although focused on the activities of fund management, the document covers some concepts that can be applied to the processing of personal data.

As for AI, the subject currently has no defined contours. As the sector’s promised legal framework has not yet been put in place, there is not even a defined regulatory process, let alone something like self-regulation. It is possible that, with the EU’s decision to approve the AI Act, Brazil will be encouraged to accelerate the creation of the a legal framework for the sector.

 1.6 System Characteristics

Brazil has adopted an “omnibus” regime for data protection: legislation of higher origin, linked to a constitutional (federal) rule, regulates security, processing and privacy issues related to personal data.

It was not easy to approve the LGPD, and it has not been easy to ensure that its standards are applied. This is due to social and cultural differences, but also to Brazil’s legislative system. This is the reason for the “omnibus” law, which helps to reduce legislative disparities and the risk of decisions that could “implode” the concepts and principles related to personal data and its protection. Brazil, unlike the EU, did not have a conceptual legacy for protecting privacy and its relationship with personal data. That is why it chose the option of a “national” law, a framework that is both engine and booster, but with a bias that inhibits local and sectoral initiatives.

Another point in favour of the Brazilian model is that, with “national” law, regulation can occur vertically or horizontally, and cover different sectors. The market may complain about Brazilian legislation, but it is undeniable that the “lex omnibus” derived more from an economic and historical context than from a government option. But there is still a long way to go. With regard to AI, NFTs, regulated businesses and so-called “paranational” relationships, EU and US regulation is more effective, deeper, and tougher. Mechanisms such as “data sharing agreements”, “joint processing treaties”, and others were not even considered in Brazil. Measures such as “external data control” and “approach supervision” are also not even discussed, and this creates a negative context for the LGPD.

 1.7 Key Developments

In the last twelve months - even though other countries have made great strides towards regulating highly relevant aspects of personal data, AI, NFTs, digital markets and other subjects – Brazil has also taken some important steps:

17 states already have internal standards that regulate the LGPD within their limits;

AI (even without a legal framework) has advanced in many sectors (facial recognition, credit granting, medical diagnoses, distance learning, and technological innovation);

the LGPD has been increasingly used in labour court rulings and consumer relations (in 2023 there were around 1,200 rulings, while in 2022 there were only around 600);

the ANPD has published the Regulation on Dosimetry and Application of Administrative Sanctions (Resolution 4/23) related to infractions involving personal data;

the ANDP published its guide for processing personal data for academic purposes and research;

discussions have begun about the “monetisation of personal data”, a controversial topic full of controversies (Bill 234/23); and

the ANPD published the updated and consolidated version of its guidance on definitions of personal data processing agents and data protection officers (DPOs).

 1.8 Significant Pending Changes, Hot Topics and Issues

In the coming months, many hot topics will be revisited. Among these are:

“monetisation of personal data”;

“sharing” personal data contracts;

“datapharma” and its regulation (sensitive data);

personal data in the banking sector;

retention of personal data codes;

self-regulation (SROs) and partial self-regulation (ASROs);

dispute resolution chambers for matters of personal data;

DPOs and work relationships;

compliance for personal data;

AI regulation;

data governance at companies;

NFTs and personal data;

personal data market and regulation; and

contracts for the representation of personal data.

Safe-Harbour Agreements and the Schrems Case

A highly significant issue concerns the decision in the Schrems case. As this case could have many future repercussions in Brazil and other countries, it is important to know a little more about it. Austrian privacy advocate Max Schrems questioned the security of the transfer of his personal data through a famous social media platform, carried out at the time under the EU-US safe-harbour agreement. Schrems argued that Edward Snowden’s revelations about US intelligence agencies indicated a lack of protection against surveillance under US law.

Therefore, the CJEU invalidated the safe harbour due to the lack of adequate safeguards required by EU law. The EU and the US then negotiated a replacement agreement (the “Privacy Shield”), created as a new recognised basis for data flows in compliance with EU law. But this second arrangement was also later invalidated by the EU. The court concluded that certain programmes that give US authorities access to personal data transferred from the EU for national security purposes create limits to the protection of that data. Such limits indicate a lack of protection that is “essentially equivalent” to EU law and means that data subjects may have no rights actionable in courts against US authorities.

One of the alternatives that emerged was the adoption of “standard clauses”, which were not invalidated by the CJEU, although the court’s recommendation was to assess, in each case, the integrity of the protection offered by them, with the possibility of adjustments or amendments.

Transfer Risk Assessments

Many countries – such as the United Kingdom, through the Information Commissioner’s Office (ICO) – have decided to adopt a very useful instrument, the transfer risk assessment (TRA). This instrument considers two alternatives: a comparison between the situation of data subjects and their data in, for example, the UK (ICO model) or a comparison of a country’s laws and practices with those in the data importer’s jurisdiction (European Data Protection Board model). This involves both knowing the extent to which personal data protection safeguards are similar to those of the domestic regime and questions of access by third parties, especially governments.

2. Fundamental Laws

 2.1 Omnibus Laws and General Requirements

The term “omnibus law” generally refers to comprehensive piece of legislation that covers a wide range of issues or policies. These laws are often enacted to simplify and consolidate laws or regulations into a single set, facilitating their implementation. General laws are typically employed to address complex or interrelated issues that may require multiple changes to existing laws.

On the topic of “personal data”, Brazil, although it has not adopted a strict “omnibus law”, uses the concept to ensure that legislation/regulation subordinate to the Constitution is always in accordance with it in all aspects. If this does not happen, the legislation/regulation will need to be changed or adjusted until it aligns with the Federal Constitution.

Data Protection Officers

The LGPD provides that organisations that process personal data must have a data protection officer (DPO). But the ANPD softened this rule (Resolution 2/22). Therefore, small data processing agents, depending on their profile, are no longer required to have a DPO. For organisations that need to have a DPO, there are some LGPD requirements that need to be met and other good practice rules. For example, the DPO must report to the company’s highest authority, have administrative and financial independence and be the link between the company and the external public.

Criteria for Data Processing

The requirements for processing personal data are all set out in the LGPD, and include everything from the collection process (what data to collect, from whom, how, in what form and for what purpose) to the process of ending the processing (return, maintenance or elimination). The LGPD also establishes where processing authorisation or consent applies, whether it is possible for the data to be shared and how its international transfer takes place.

“Privacy by Design/Default”

These principles are already found, at least in essence, in the LGPD, especially because it aims to ensure that the privacy of data subjects is guaranteed and protected from the beginning, without relying on third parties who have detailed knowledge or understanding of privacy settings. This gives data subjects greater control over their personal data and helps prevent unauthorised access or unwanted use of their data.

Impact Analysis and Privacy Policies

The LGPD has rules that aim to ensure that the processing of personal data is specifically fair, for a lawful purpose, on an authorised legal basis and dependent (if applicable) on a legitimate interest assessment (LIA), the analysis that allows determining whether data processing can even occur based on legitimate interest.

Data Subject Access Rights, Anonymisation and Pseudonymisation, Big Data and AI

One of the principle of the LGPD is that the data subject always has control and ownership of their personal data. This means that they, and only they, can guide the controller over what is possible and what is prohibited to do with their data. This is why the LGPD guarantees data subjects the right to determine the fate of their personal data, as they never lose ownership. For example, it is the data subject who decides on anonymisation, erasure, alteration, storage, and other actions involving their data.

Injury/Harm

As the Constitution establishes the firm concept that personal data is the property of the data subject and that its protection is a fundamental right, any injury (or threat) to this data is treated seriously and data has a high level of protection. Personal data involves material, emotional, financial, reputational, intimate, and family aspects, and an injury (or threat) to personal data represents, in practice, an injury (or threat) to the concept of individual dignity, which deserves the protection that governments give it.

 2.2 Sectoral and Special Issues

Ordinary and Sensitive Data

Under Brazilian legislation, personal data falls into two categories: ordinary and sensitive. Ordinary data is “common” data that does not intensely affect the privacy or intimacy of its subject. Sensitive data, on the contrary, is data with a greater degree of intimacy and therefore carries a greater need for protection for the subject. Different or intermediate degrees (such as data relating to financial, academic or previous criminal activity) have not yet been included in the legislation.

Ordinary data has “ordinary” protection, that is, common protection; sensitive data has “special” protection, and its processing can only be carried out under specific conditions. For example, ordinary data can be processed if there is a legitimate interest, and this allows for an open range of possibilities; but sensitive data cannot be processed under a legitimate interest, other legal bases applying to them (Article 11, LGPD).

There is a risk that has become common among data controllers: assigning ordinary data the status of sensitive data, just because it seems that certain data, by its nature, “should” be considered sensitive. In principle, the decision is nothing unusual. But it is necessary to remember that if the controller itself decides to reclassify certain data, from ordinary to sensitive, its decision is incorporated into its internal practice, and this is incorporated into its policy, even without a written rule. This means that, after making this decision, it is not possible to go back, and its effects can complicate things for the controller.

Command Data

Although national legislation only talks about common and sensitive personal data, there is a category of data that can complicate things. This is what is known as “command data”. This class includes elements such as tracking, image capture, targeted advertising, active location, behaviour in the media and social networks, provoked responses or comments, among others. Command data is so-called because it is not always personal data generated by the holder, but derived from an external action that leads the holder to produce data that it did not have before that action. This type of data has been gaining in importance, and the tendency is for legislation to also provide it with protection.

Privacy and Public Safety/Public Interest

The LGPD provides that data associated with these practices can be processed for the purposes of applying criminal sanctions, which signals that, in this case – as the Superior Court of Justice of Brazil recently decided – the collective or social value can outweigh the individual value.

The Right To Be Forgotten

The Supreme Court (RE 1,010,606) has found that the right to be forgotten is not compatible with Brazilian law, and for this reason argued that the passage of time, in isolation, is not a reason to prevent facts from being publicly disclosed.

 2.3 Online Marketing

The boundaries between unsolicited communications and irregular processing of personal data are conceptual rather than concrete. In the EU, “consumption access” may require authorisation (not consent) from recipients, and recommendations continue to be that an individual’s email should not be used for mass communications or pre-ticked boxes for authorisation.

Brazil is preparing to regulate the practice, but only the State of São Paulo (Law 17,334/21) has rules to prevent unwanted calls and unsolicited commercial messages (or active capture of preferences and profiles). In any case, the Consumer Protection Code (Law 8,038, article 39, III) establishes that the supply of unsolicited goods or services is an “abusive practice” and prohibited. Recently, Bill 310/22 went further: it prohibits telemarketing companies from unwanted contact with people, including automated calls.

Targeted advertising, especially towards more vulnerable people, such as children and the elderly, is also considered abusive and prohibited by consumer law.

 2.4 Workplace Privacy

The work environment benefits from the concept of privacy. But, in times of remote or hybrid work, it is not simple to define the “workplace”, as it can be the physical environment or a place where the worker performs tasks (home or public place). The consensus seems to indicate that the typical “workplace” is the physical location of the company where the worker provides services.

Companies have been increasingly concerned about personal data privacy in this case, as workers, even outside their physical locations, also need to manage data for their activities. Therefore, the number of companies that have been adopting strict control and privacy policies when processing personal data outside their facilities is only growing, with the signing of confidentiality and non-disclosure terms, digital security commitments and secure data management and information.

Codes of conduct and integrity in personal data privacy and internal personal data processing notices have also become common and there is almost always no inclination that these violate workers’ privacy. The Brazilian Labour Court has already made it clear that employees have an obligation not to violate the personal data of third parties, especially if this is what is expected of their activities in the company.

Another point of caution is that workers who manipulate large masses of personal data in their activities are always subject to paid external capture so that they provide (or facilitate access to) strategic data (personal or not) to the employer’s competitors or to people who are dedicated to predatory practices. It is true that Brazilian legislation allows organisations to adopt measures, technological or otherwise, to protect their strategic information and the personal data it processes. But it is also true that a significant number of organisations have not yet adequately prepared themselves for this.

As for AI guidelines, Brazil is expected to have a legal framework in place for AI in the coming months, based on ongoing legislative proposals. For now, events related to AI, in the workplace, can be conducted based on the Internet Legal Framework and the LGPD, according to the rules that are applicable.

 2.5 Enforcement and Litigation

Brazilian regulators have at their disposal a group of mechanisms to open investigations into violations of personal data guarantee, security, and privacy laws.

According to the LGPD, the ANPD can directly interfere in an organisation’s data processing activities. This can be done in three ways:

active regulatory intervention, if the controller has been accused of systematically violating the rights of the personal data subject;

suspensive intervention (Article 52, X); and

punitive intervention.

In general, the regulator initiates an investigation against the processing agent and assesses the nature and severity of the infractions committed, ensuring a full defence and production of evidence. The main basis for this is the “conduct of the processing agent”, the actions and measures it adopted – or failed to adopt – (which led to the vulnerability of its controls) and the documentation in data processing. Therefore, before even proving the infringement, the regulator can consider the nature and severity of the conduct as a way of arriving at the most appropriate legal assessment.

Classification and Penalties

In general, the regulator considers violations to be direct or indirect, and may include cross-cutting violations. The direct ones result objectively from the agent’s conduct, the indirect ones result from the worsening of the effects of its conduct and the transversal ones consider the impact of the violation on other agents and regulators.

The regulator can also apply penalties provided for in the LGPD, generally in the “verticalisation” regime (from least serious to most serious). Even penalties may vary depending on the nature and quality of the infraction, because if the same infraction can be considered and punished by more than one regulator, it is possible that the original penalty will be aggravated by a secondary regulator (which does not directly regulate personal data).

Class Actions

Private legal disputes over violations of privacy or intimacy are common, including through so-called collective actions, in which different actors come together to protect rights or discuss legal duties that apply to everyone. Collective defence entities have been concerned with the issue of “indistinct privacy” or “collective privacy”. In this case, there are no specific individuals affected by a privacy breach, but an indistinct group of them.

This is the case of personal data leaks. Consumer relations organisations and the Public Prosecutor’s Office have taken a stand on it, especially in relation to data leaks related to payment arrangements articulated by the Central Bank. This is of particular relevance as Brazil is the fourth preferred global target for personal data breaches.

3. Law Enforcement and National Security Access and Surveillance

 3.1 Laws and Standards for Access to Data for Serious Crimes

Article 4, III, of the LGPD establishes the so-called “exclusionary principle”. In short, this Article states that the LGPD rules have restricted application when the subject is the processing of personal data related exclusively to public security, national defence, State security or investigation and repression of criminal offences.

Therefore, if data processing is related to these purposes, it will not be fully subject to the LGPD, and the government will not necessarily be obliged to ask the regulator for access to databases of crimes, infractions, and related processes. This does not mean that the authority accessing the data is entirely free to use it as its wishes. This is because another principle of the LGPD, “purpose”, establishes that, once the government declares that access to data is related to the repression of crimes and infractions, it cannot change this purpose to another. For example, the LGPD says that the public administration that accesses the data cannot transfer it to third parties, with exceptions, and that the regulator can act against the government if it violates this legal assumption.

Another aspect to be considered is that the public authority that wants to have access to data in cases of repression of crimes and infractions can go directly to the judiciary, without going through the regulator. But this creates a problem: special instance suppression. Once there is a regulator, only if it refuses to allow access to data can the government ask the judiciary to act on the case.

 3.2 Laws and Standards for Access to Data for National Security Purposes

The issue of “national security” is a problem that has not yet been legally resolved in Brazil. This is an “open concept”, which allows for multiple interpretations, and this lack of definition on Brazil’s part has placed the country in a delicate situation before the world and some organisations, such as the OECD.

The LGPD itself does not have clear rules on the handling of personal data when it comes to “national security”. For example, Article 4 speaks, ambiguously, of “national defence”, a concept that is not always the same as “national security”, which is much broader.

The current situation is that the LGPD (Article 4, III) does not fully apply if the processing of personal data is objectively related to “national defence” and “state security”. In principle, if data processing is intended for one of these purposes, the public agent is not subject to the LGPD, and therefore does not need authorisation from the regulator to access intelligence, state defence or “national security” databases.

As for the OECD, Brazil, although invited to join this entity, has not yet met all the necessary conditions. But the arguments continue, even though the matter is not on the list of priorities of the current government.

 3.3 Invoking Foreign Government Obligations

Brazil has joined the Budapest Convention on Cybercrime. The document requires each country to maintain the legal authority to compel organisations in its territory to disclose data (including personal) that is in their custody, regardless of whether the organisation also has custody of data from other countries.

This means that Brazil must, even without adhering to an agreement on the free movement of personal data for certain purposes (such as the American Cloud Act), examine requests for data capture and transfer. The Cloud Act (Lawful Use of Data Abroad Clarification Act), passed in 2018 by the United States Congress, is basically the result of the limits of the Stored Communications Act (1986). It determines that US data and communications companies must allow access to customer data, even if their repositories are outside US jurisdiction. This created a problem for the GDPR, which, after the Cloud Law, linked access to data stored in a foreign country to prior judicial authorisation from that country. See 1.8 Significant Pending Changes, Hot Topics and Issues (Safe-Harbour Agreements and the Schrems Case).

But a foreign government’s request based on the Budapest Convention, or an agreement like the Cloud Act, does not indiscriminately give a private organisation the right to request access to personal data included in the government’s request. This organisation, based in Brazil or another country, needs to use its own means to access the personal data it desires, and is subject to scrutiny by legislation and the judiciary.

 3.4 Key Privacy Issues, Conflicts and Public Debates

Privacy and Data Monetisation

The topic of citizen privacy is gaining more and more attention, and debates around it have featured in Brazilian media. One of these issues relates to “data monetisation”, which basically means that an organisation can “commercialise” its database, thus obtaining a financial return. As data (and not just personal data) is an extremely valuable asset (sometimes referred to as virtual gold), monetising it can be advantageous. But what are the limits? What kind of rules can protect the data subject from a leak? How to protect it from the phenomenon of “dispersion” (when data is spread out in such a way that its control becomes, in practice, impossible)?

Agreements Between the State and the Private Sector

Another debate involves the government, which, discreetly, has signed agreements with private entities and representatives of business sectors. The Central Bank, for example, signed co-operation agreements with private entities representing financial institutions. These agreements provide authority for the Central Bank to share a large database (National Civil Identity), which includes sensitive data, such as biometrics. The Federal Public Ministry is investigating the matter, and representations were made, including to the Federal Audit Court (TCU), which found no irregularities in the agreements.

4. International Considerations

 4.1 Restrictions on International Data Issues

The international transfer of personal data is a topic to be considered carefully. Such transfers may indicate that data, once out of national jurisdiction, is “lost” (or dispersed) forever, especially in regulatory terms.

In the LGPD, international transfers are an exception, both active (from Brazil to abroad) and passive (from abroad to Brazil). Such transfer, according to the LGPD, is only possible:

if items II, V and VI of Article 7 of the LGPD are met;

if necessary for international legal co-operation between public intelligence, investigation, and prosecution agencies;

if necessary for the execution of public order or the legal assignment of public service;

if the controller provides and proves a guarantee of compliance with the principles, rights of the data subject and the personal data protection regime provided for under the law;

if the data subject gives their consent;

if the ANDP authorises it;

to countries or international organisations that guarantee an adequate level of data protection (similar) to that provided for in the LGPD;

when intended to protect the life or physical safety of the holder or third parties; and/or

when it is the result of a commitment under an international co-operation agreement.

Importing data via international transfer is possible based on:

data filters;

formalisation;

judicialisation of the transfer – this is not treatment subject to the LGPD, (Article 4, IV)

source conformity level;

the use of transfer; and

verification of Brazilian destination.

 4.2 Mechanisms or Derogations That Apply to International Data Transfers

The international transfer of personal data, according to the LGPD (and the GDPR), is a typical data processing activity and must meet legal conditions, including derogations (specific authorisations that consider knowledge of the risks involved).

These conditions include that the transfer:

cannot include more data than necessary;

must be done on a legal basis;

must be naturally informed;

must be subject to one of the derogation possibilities (LGPD, Article 33 or GDPR, Article 9, Section 2);

must be subject to real measures to protect and contain risks; and

must have a fair, legitimate and non-prohibited purpose.

As for multilateral mechanisms, the transfer (especially international) of personal data must be regulated in a Personal Data Transfer Agreement (PDTA), with rules that guarantee the bilaterality of the data communication contract. Additionally, a data privacy notice is highly recommended.

 4.3 Government Notifications and Approvals

The legal hypotheses that allow the international transfer of personal data are in the LGPD (Article 33). The transfer cannot be made without these derogations.

One of these hypotheses establishes that the regulatory body can authorise the transfer, but this requires that the event meets one of the legal bases of the LGPD. Although the government has decided to carry out an international transfer of data, the case must fall within Article 33 of the LGPD, and even then, it is up to the regulator to evaluate the “transfer conditions”, provided for in Article 35.

In general, public persons referred to in the Access to Information Law (Article 1) may request the regulator, before international data transfer, to assess the degree of data protection afforded by the country or international organisation that will receive the material.

 4.4 Data Localisation Requirements

Regarding personal data localisation, a point of interest is that Brazilian legislation has adopted the “principle of irrelevance of location” (Article 3). The point where the data is located (or stored) is not significant for law enforcement.

But this depends on the following conditions:

the personal data to be processed is collected in Brazil;

the processing operation must be carried out in the national territory; and

the purpose of the processing activity is to offer or supply goods or services, or process the data of natural persons located in the national territory

Data that, due to its nature, purpose, quality, scope, and content, must remain in Brazil, cannot be transferred, such as personal data used by research bodies in public health studies (LGPD, Article 13, Section 2).

 4.5 Sharing Technical Details

The sharing of personal data with third parties is an exception to the usual obligations on a data controller, because this data should normally remain under its custody, so that the data subject’s privacy is protected. But, if sharing is necessary, some rules must be observed. GDPR rules require that all data subjects be encrypted, which includes thinking about security systems for managing keys. Under the LGPD, there is no obligation for encryption, but a requirement that secure techniques be put into practice to make personal data unintelligible, and the most obvious solution to such a requirement is encryption.

There are no explicit rules in the LGPD on how key elements (source codes, software and other technical data) should be shared with the government, this subject requires further regulatory guidance in Brazil.

It is possible for public and private entities to share personal data, as long as they comply with Article 25 of the LGPD and the data is used for public purposes, in the public interest, in the exercise of legal powers or in the fulfilment of legal public service duties.

In addition, sharing does not necessarily mean a violation of copyright protection, as algorithms, for example, are not always seen as “intellectual products” (Law 9,610/98, Article  8, I). But it is necessary to consider that sharing typical intellectual creations – such as source codes – can lead to legal disputes (Law 9,609/98, Article 2, paragraph 5).

 4.6 Limitations and Considerations

Agents who collect or transfer personal data in connection with requests from a foreign government are subject to the LGPD, provided that the data was collected in Brazil and that at least one processing activity was carried out in the country (Article 3). According to Article 3 of the LGPD, it is irrelevant whether the agent is located in Brazil or abroad, as what establishes the application of Brazilian data law is the place where the data was collected and where it was subjected to processing. In the case of an international data transfer between an organisation and the entity that contracted it, however, the transferee is subject to the LGPD transfer rules – ie, a legal basis (Articles 7 and 11) and a purpose will be required, in accordance with Article 33 of the LGPD.

 4.7 "Blocking" Statutes

This type of statute is becoming increasingly widespread, and its rules provide for limitations that, if they do not prevent practices involving personal data, create conditions that processing agents must comply with before acting.

Even though blocks are not always related to the protection, security and privacy of personal data (as this is not always the focus), it is undeniable that one of their effects is to create difficulties for practices that would otherwise be permitted.

An example is the EU GDPR, which has already been seen as a blocking tool for transfers of personal data to non-EU agencies (applying Article 49(1)(d)) when it comes to “important reasons of public interest”.

This was made most evident by the US District Court decision (2019), which calls for an answer as to whether the GDPR is in fact a blocking statute under US law.

5. Emerging Digital and Technology Issues

 5.1 Addressing Current Issues in Law

Some of these topics are addressed, directly or indirectly, by the LGPD, such as facial recognition, biometrics, pictorial data processing, personal distinction, profiles, metadata and reverse data.

Drones

There is still no specific comprehensive legislation on drones in Brazil. Some standards (such as Special Civil Aviation Regulation 94/2017 of the National Civil Aviation Agency) try to overcome this gap, especially regarding the need to preserve the private life and intimacy of individuals.

Big Data

The mass (intensive) acquisition of personal data is strongly impacted by the LGPD. Article 20 establishes that it is the data subject’s right not only to know on what legal basis decisions were made regarding them, but also to request corrections, changes and repair of abuses.

AI and IoT

Law 14,108 (the “IoT Law”) is not the legal framework for the subject, but it creates government incentives for technologies focused on IoT. Brazil does not yet have a legal or regulatory framework for AI. At this moment, the most relevant and current initiative is Bill 2,338/23.

Dark Patterns (DPs)

Dark Patterns are user interface elements that, through attention items, colours, positioning, flashing elements and other artificial techniques, try to induce the individual to opt for something that, in fact, they did not want or would like to buy or use.

The Consumer Protection Code conceives of dark patterns as a type of misleading advertising. This is because this Code establishes that it is the consumer’s basic right to have access to “adequate and clear information about different products” and determines that “coercive or unfair commercial methods”, which include obscure patterns, are abusive and illegal.

Profiling or Micro-targeting

The subject of “profiling” has been under discussion for years, but only with privacy laws has its relevance become evident. For the GDPR, “profiling” is “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular, to analyse or predict aspects concerning the work of that natural person, their economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.

The Brazilian data law, the LGPD, goes even further, and says that personal data is considered to be any data used in generating the profile of an identified person (Article 12). This means that the elements that form the profile, and the profile itself, can be under the protection of the law, including the rights and duties it establishes, as stated in the LGPD (Article 20).

But is it just the formation of a profile that must comply with legislation? It seems clear that profiling, as well as its potential variations (microtargeting, etc), since they are based on the same principles and concepts (tagging people with a defined objective), must be evaluated under data protection legislation.

Fiduciary Duty

Brazilian legislation states that a bond is formed between the controller and the holder, and this requires the controller not only to comply with the legislation, but also not to frustrate the legitimate expectations of the holder.

 5.2 “Digital Governance” or Fair Data Practice Review Boards

Brazil does not yet have specific regulations on digital governance (or on personal data, or AI) and nor has it implemented a regular practice in this field, even though the LGPD provides one (under Article 50) and recommends the introduction of general governance practices in organisations.

In fact, organisations create governance committees themselves, generally linked to their DPO, so that issues such as risks, compliance, standards, management and documentation can be addressed on a legal and technical basis.

 5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

There are no specific cases on the protection of personal data involving repercussions and penalties in Brazil’s recent history. However, it is worth remembering that the number of lawsuits related to this issue is only increasing, and has now reached the thousands, which means that the ANPD, at some point, will need to get involved in these cases.

 5.4 Due Diligence

Talking about personal data and its protection in Brazil is still new, but a good number of due diligence processes are starting to value the search for compliance in the processing of personal data related to transactions between companies.

Cases of investment planning and strategic partnerships are requiring partner, invested, or synergistic companies to present a compliance diagnosis related to the LGPD and, in several cases, a diagnosis connected to the GDPR.

This may include:

analysis of operators and sub-operators;

collection of data protection documents (policies, procedures, protocols, and guidelines);

consultation on the history of incidents involving personal data and communications to the ANPD, other regulatory bodies, and data holders;

information on judicial or administrative proceedings relating to the LGPD;

measurement of the flow of service to the demands of holders and those involved in the service;

the value of personal data;

the value of the need to comply with other laws in international transfers;

the value of the systems used in processing activities;

verification of the privacy framework, whether there is a DPO, and a privacy committee; and

verification of the technical and organisational measures adopted in the processing of personal data.

 5.5 Public Disclosure

There is still no specific legislation in Brazil that requires disclosure of an organisation’s cybersecurity risk profile.

This can be explained as follows: in personal data protection, the country needs to make progress before instituting a cybersecurity or personal data security classification; and this classification depends on the maturity of data security and privacy concepts and principles.

The activities of assessing, measuring and monetising the risks of processing personal data are new in the country, and the criteria are not yet very clear. One example is vulnerability analysis for classes and categories of manipulated data. This kind of analysis evaluates four pillars: compliance with legislation and safety standards, blank spaces for security incidents, resilience to potential threats (internal and external), and protection systems implemented.

 5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

Key trends in terms of data protection and privacy (including in regard to personal data) include the following.

The Digital Services Act (DSA) has started to apply to online platforms and large search engines. In Brazil, a similar law is being discussed, which would act on open and closed digital markets (NFTs, certificates, electronic business chains, among others).

A Bill on the AI Legal Framework is under discussion, and everything indicates that it will be accelerated by the approval of the AI Act in the EU. This indicates that many important concepts will be incorporated into the framework, such as the principles of “innovation” and “logical precision”.

The ANDP is considering approving specific rules on the sharing of personal data (including sensitive ones, under certain conditions) between controllers, in order to reduce the risks of data dispersion.

 5.7 Other Significant Issues

The most significant topics for data protection regulation in Brazil include:

data processing in environments regulated by other authorities;

DPO technical and operational standards policies;

leading security incident investigations in the case of agents and members of different organisations;

massive (intensive) data processing (regulation and limits);

monetisation and demonetisation of personal data;

permanent international transfer of personal data;

personal data as a legacy in international transactions;

service level agreements on personal data processing compliance; and

sharing of public databases and their effects.

159. [Artificial Intelligence: What is it and Can it Help My Business?](https://lawpath.com.au/blog/artificial-intelligence-what-is-it-and-can-it-help-my-business)

What is Artificial Intelligence?

Artificial intelligence is the science and engineering of creating intelligent machines, particularly intelligent computer programs. In general, these intelligent programs are able to understand large amounts of data. The main purpose for doing so, is to solve complex problems, make decisions and make predictions based off that data. Importantly, they can do this on an expansive scale. In this way, AI is constantly learning, just like humans. Also, the capabilities are virtually endless for AI machines and in recent years, the [AI community](https://www.industry.gov.au/policies-and-initiatives/artificial-intelligence) have made leaps and bounds in their development and innovation.

Examples of Artificial Intelligence

We all interact with some form of artificial intelligence on a daily basis. It’s not just about high-tech machines and robots. Do you own you use a Smart Assistant, such as Siri or Alexa? Maybe you own a self-driving car? Do you use Netflix, Facebook, TikTok and other social media platforms? Maybe you own a robot vaccum cleaning? Well, all of these examples are a type of AI. For instance, social media platforms and Netflix use a variety of algorithms to understand your interests and show you content on that basis.

How Artificial Intelligence can help your business

Artificial intelligence has a great usage across many types of businesses. Now, AI is not going to replace your employees jobs. But, it will make their jobs a lot easier. Many companies and firms within the [legal industry](https://lawpath.com.au/blog/how-can-artificial-intelligence-be-used-in-the-legal-industry) are already utilising the benefits that AI has to offer. Below, we’ll take you through just a few ways AI systems can be used to improve your businesses efficiency.

Customer Service

A variety of businesses use online Chatbots. It’s basically an automated assistant that offers to answer your many questions, and they can! Many Chatbots have the capability of answering a customers questions in a matter of seconds. Therefore, Chatbots are able to understand your customers problems and provide a quick and relevant solution or answer. Thus, they can help improve the efficiency of your businesses customer service, ensuring no customer is left waiting for a response.

Speech Recognition

We are all aware that Siri and Alexia have been making their way into many Australian homes. But, what about the workplace? Well, speech recognition can be a valuable tool if your business is strong on writing and communication. Specifically, speech recognition programs can aid in speeding up your businesses writing process by using verbal cues, demands and sentences. Saving you valuable time to work on more pressing tasks.

Increased Data and Information Security

AI can be implemented into your workplace to increase your businesses security systems. Therefore, you don’t need to be worrying about whether your businesses security is going to be breached, and data is going to be leaked. AI can improve your systems and allow your business to live up to its policies around data and information, including your [privacy policy](https://lawpath.com.au/legal-documents/privacy-policy). AI systems are to able to detected when a breach may occur, before it has occurred. Thus, improving the quality and security of your businesses privacy and data.

Key Takeaways

There is no doubt that artificial intelligence has gained increased popularity and momentum in recent years. But, AI is so much more than robots. Many of us already interact with a variety of AI systems on a daily basis. Possibly without even realising. In general, artificial intelligence can be defined as a machine or program with the capabilities of understanding large amounts of data, and giving a specific and tailored result. Many businesses have even opted to use AI tools to help with their businesses tasks and operations. You can too!

160. [Webber Wentzel embraces Generative AI as part of its ongoing innovation journey](https://www.webberwentzel.com/News/Pages/webber-wentzel-embraces-generative-ai-as-part-of-its-ongoing-innovation-journey.aspx)

While Webber Wentzel has been engaged in AI innovation for some time, it recognises that generative AI is the next frontier and warrants a prioritised and purposeful response from the firm.

The firm has dedicated significant resources to explore, pilot and embed ​generative AI into its business, with a parallel focus on continuous learning and empowerment of employees. This commitment will allow the firm to remain at the forefront of AI applications in law, ensuring that their clients and employees benefit from the most advanced and effective legal technologies.

"We are excited about the transformative potential of generative AI and the efficiencies it can bring to our business. We are following a pioneering but responsible approach to AI innovation, carefully balancing the opportunities with the associated risks and challenges" said [Sally Hutton](https://www.webberwentzel.com/Specialists/Pages/sally-hutton.aspx), Managing Partner.

Webber Wentzel has adopted an investment framework that is tailored to its strategic priorities, the nuances of its business and the legal services sector, and the potential risks presented by the technology and in June 2023, adopted a formal generative AI policy.

The firm's generative AI policy has been carefully crafted to safeguard the interests of the firm's clients, addressing confidentiality, data security and intellectual property concerns, and ensuring that the firm's use of generative AI is always strictly within legal and ethical bounds.

"We are applying an investment mindset that is both forward-thinking and grounded in pragmatism and long-term sustainability. We recognise that generative AI is not a magic bullet. We are committed to choosing the right legal technology for each unique use case to scale our expertise and capability, with the aim of providing a top-tier experience that exceeds the expectations of both our clients and people," said [Aalia Manie](https://www.webberwentzel.com/Specialists/Pages/Aalia-Manie.aspx)​​, Head of Legal Solutions & Technology.

Webber Wentzel's AI investment approach reinforces its position as an leader in legal innovation in Africa, demonstrating a keen commitment to both technological advancement and legal and ethical responsibilities, and ensuring that the firm continues to shape and practise the future of law, today.

​161. [Responsible AI: embracing generative artificial intelligence technologies- a brief guide for organisations](https://www.ensafrica.com/news/detail/7109/responsible-ai-embracing-generative-artificia)

Responsible AI: embracing generative artificial intelligence technologies- a brief guide for organisations

With the boom of ChatGPT, AI frenzy, and similar technologies ("generative AI") companies are questioning whether to allow their staff to utilise Generative AI for company purposes and if so, how to regulate such usage in order to minimise legal risk, especially in the absence of regulation in most jurisdictions.

Whilst some companies have adopted the view that they will not allow staff to utilise generative AI (which in itself is risky), for companies that are looking to leverage the benefits of generative AI in a responsible manner, we would recommend that such companies institute a number of measures. Before we expand on what measures companies should seek to adopt, we start with a short discussion on the risks around the usage of generative AI.

Generative AI technologies risks

ChatGPT and other generative AI technologies expose companies to a myriad of risks including:

Corporate governance and accountability – In South Africa, King IV places an imperative on company boards to ensure sound information governance and sound data governance. The adoption of generative AI technologies should therefore be lead by the board as opposed to allowing employees usage to be unchecked. This also ties in with the condition of accountability under the Protection of Personal Information Act, 2013;

Confidentiality – as the majority of AI technologies are owned by third parties, a company risks its employees disclosing confidential information or trade secrets to unauthorised parties;

Cybersecurity – if any confidential information is disclosed, it will be stored in third party databases. If a hacker breaches the database, there is a risk that the company's sensitive information could be unlawfully accessed;

Data privacy and protection – a company should list the categories of confidential or sensitive information which employees may not upload or use when accessing AI technologies;

Intellectual Property – a company should clearly indicate its ownership over its data and outputs generated by Generative AI technologies (provided that it is the company and not a third party is entitled to ownership over such outputs);

Regulatory compliance – a company needs to ensure that its storage and processing of data or personal information is in accordance with applicable laws;

Liability – the use of AI could give rise to claims from a number of sources including clients, users, third parties, and even regulators;

Contracting – as companies would inevitably rely on third party service providers to provide skills as well as tools, companies should ensure that agreements with such service providers do not include any exclusion of liability and/or restrictive liability provisions;

Data bias and discrimination – any biases in the company's data could to an AI reinforcing stereotypes, discriminating against people, or creating exclusionary norms;

Outdated or inaccurate information and misinformation – a company relying on generative AI runs the risk that the information used by the AI might be outdated or inaccurate which could lead to incorrect responses being generated. Companies also face the risk of their AI being a target of misinformation campaigns; and

Unqualified advice – if employees use generative AI to generate advice and provide such advice to clients without review, it could lead to a situation where advice has been given by unauthorised entity.

What if my organisation does nothing?

If a company's stance on AI in the workplace is prohibitive or silent, it could lead to a situation of shadow IT. Shadow IT, is an organisational challenge, where employees adopt a technology which is not implemented or deployed by the company. If companies ban ChatGPT and other generative AI technologies, employees could resort to secretively utilising such technologies. This would further compound the company’s risk as it would not be able to regulate or even monitor employee usage of AI. It is recommended that companies adopt a policy to address and regulate AI use in the workplace in order to mitigate some of the abovementioned issues.

What interventions can a company institute?

Whilst there is not a once-size-fits-all approach when it comes to the type of interventions to be instituted, as this would be largely dependent on the scope of usage of generative AI in the company's operations, in the absence of interventions, some of our suggestions include:

Governance: the board needs to ensure that proper structures are put in place as well as safeguards employed in order to ensure the adoption of Responsible AI. These may include establishing Centres of Excellence, dedicated task teams, and or other structures whose focus is ensuring that AI is adopted in a Responsible manner in keeping with the values and culture of the company and also in order to mitigate legal, technical and financial risk;

Policy implementation: a sound policy for the adoption of Responsible AI needs to be implemented. These would include not only mechanisms to mitigate legal, technical and financial risk but also ensure that ethical boundaries have been established based on the company's own value system;

Training: companies should ensure that staff are trained at various levels and that training be adapted depending on what role staff members undertake as part of the company's AI initiatives. Example: (i) legal and technical teams should undergo training on more than just the legal and technical risk of AI adoption but also on AI ethics and financial risks; and (ii) board of directors need to be trained on both ethical and legal considerations in order to establish a culture of Responsible AI;

Contracting – as companies would rely on third party service providers in order to deploy AI solutions, companies should ensure that they establish sound contracting standards in order to mitigate against the risk of a supplier providing tools and/or solutions which may give rise to claims and such supplier not being liable due to restrictive liability provisions. Further, the usual due diligence in supplier selection needs to also be adopted;

Ethical impact assessments: Although not mandatory, it is a useful tool to ensure that any projects undertaken or AI being adopted complies with the company's policies and applicable laws;

Ethical reviews: as part of this, companies may wish to establish a distinct AI ethics review board, which would also engage in the approval of projects based on ethical impact assessments undertaken.

Pioneering industry initiatives or codes of conduct: leading companies may wish to pioneer the adoption of industry acceptable codes of conduct, including obtaining approvals from regulatory authorities such as the Information Regulator; and

Auditing and monitoring: as with any compliance initiative, boards should ensure that proper resources are dedicated to ensuring compliance with interventions adopted, as well as dealing with violates of company policies.

Regardless of whether a company deploys or utilises AI technologies in the workplace, it should ensure that it has adopted mechanisms for Responsible AI interventions and that such interventions are led from the very top.

The adoption of Responsible AI comes with several complexities, and expert guidance is often crucial in this process. In order to assist clients in fast tracking the adoption of Responsible AI, our expert TMT team have developed an AI Toolkit. We would strongly urge companies to engage with us in order to ensure that AI adoption is done so in a Responsible manner and that company risks are mitigated. For more information on our AI Toolkit, please contact: