As we increasingly rely on tools powered by generative artificial intelligence (AI), it is important to consider the potential risks and threats that come with these technologies. While these tools, and the large language (LLM) models that power them, have revolutionised the digital industry, they also present security and privacy concerns.

Ongoing lawsuits involving industry giants such as OpenAI [1], Meta [2], and Stability AI [3], or the recent passing of the EU AI Act [4], underscore the importance of enterprises seeking solutions that respect intellectual property rights and guarantee protection of corporate data. It is necessary for a company wishing to utilize AI-based tools and solutions to be aware of the threats resulting from their use.

Threat vectors

The multitude of tools based on artificial intelligence and associated benefits encourage their use in business. These tools allow you to style text, prepare reports or search documents. Coding assistants installed directly in the integrated development environment (IDE) are gaining popularity among programmers. However, their use involves certain risks that must be considered when deciding to use them on behalf of a company. One of the most important is the sharing of information with third parties.

// Sending data to the cloud

Coding assistants used from the IDE need an input to generate a response, which may include:

- contents of the open file;
- chat history;
- imported files or libraries;
- terminal window;
- indexed parts of the entire repository.

The developer must be aware that this data leaves his local machine and ensure that the data is encrypted by the assistant before being sent to the cloud. Some assistant vendors allow the tool to be run in a VPC, on-premises, or even in a fully isolated private installation to ensure greater control.

It is also worth checking whether the AI tool complies with standards such as:

- GDPR - comprehensive privacy law that requires organizations to protect the personal data and privacy of EU citizens for transactions that occur within EU member states, regardless of the organisation's location;
- SOC2 - comprehensive reporting framework by the AICPA for assessing and testing controls related to security, availability, processing integrity, confidentiality, and privacy in service organisations, ensuring robust data protection and compliance;
- CCPA - state law enacted in 2020 that protects Californians' privacy rights regarding their personal information, giving them the ability to request access to, deletion of, or prevention of the sale of their personal data, and imposing penalties for non-compliance;

[1] https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html
[2] https://www.nytimes.com/2023/07/10/arts/sarah-silverman-lawsuit-openai-meta.html
[3] https://www.lexology.com/library/detail.aspx?g=b2d22903-073f-44ce-9f7a-d07e51cad96d
[4] https://www.euractiv.com/section/artificial-intelligence/news/europes-landmark-ai-act-passes-parliament-vote/

// Context processing by language models

The prompt sent to the cloud may contain protected intellectual property, and the user/company should ensure that this data is only used to generate the response by the AI model. Most coding assistant vendors have introduced a "zero-retention policy". It is almost always available in paid plans: immediately after generating the response, the context sent from the end device is discarded and no part of it is used by the vendor or third-party.

// Keeping your data private

Context discarding should also ensure that the code available to the assistant will not be used to improve product quality. In most paid plans this is clearly stated along with the information that LLM inquiries will not be reviewed by the solution provider's employees or used for training, assessing and fine-tuning the model.

// Telemetry

Tool providers also advise on collected telemetry data, which includes statistics on the programming languages used, the rate of accepted responses, CPU and RAM available on the end device and the IDE used. This data helps determine the direction of the assistant's future development.

Intellectual Property

Huge data sets with source code are needed to train LLMs that assist software developers. Legislation still does not specify how to license the code generated by the assistant. The definition of copyright varies around the world, but almost everywhere meaningful human involvement is required. At this time, it is not clearly defined whether the person preparing the input prompt has IP rights to the output generated by AI.

Ongoing court cases regarding the use of protected intellectual property to train a model encourage companies to be cautious about using them in business processes. The organisation should minimise the risk of copyright infringement by paying attention to the licenses of the data used for training.

// Copyright infringement protection

AI tool providers offer various methods of protection against copyright infringement.

// Copyright shield

OpenAI [5] and Google [6] introduced “Copyright Shield”, guaranteeing support in case of a lawsuit against their clients. Copyright Shield applies to generally available features of enterprise API and developer platforms. It specifically covers AI-generated content that falls within the scope of copyright claims.

// Code referencing

Copilot has introduced “code referencing” [7] functionality, currently in public beta. When a user receives a code suggestion from GitHub Copilot, the system checks the surrounding code (about 150 characters) to see if it matches any public code on GitHub. If a match is found, a notification appears in the editor, showing the matching code snippet, a list of repositories where that code appears and the license governing each repository.

[5] https://openai.com/blog/new-models-and-developer-products-announced-at-devday
[6] https://cloud.google.com/blog/products/ai-machine-learning/protecting-customers-with-generative-ai-indemnification
[7] https://github.blog/2023-08-03-introducing-code-referencing-for-github-copilot/

// Open source trained LLM

Some vendors offer models trained on datasets based on open-source licenses, that do not include GPL or other Copyleft code. This is a well-thought-out solution, especially in the context of disputes regarding the licensing of code generated by a tool trained on datasets with more stringent licenses.

Legislation

Taking measures to prevent intellectual property infringement and minimising the risks arising from the use of external tools are important when using AI. One should also ensure compliance with applicable law. Consult Red has offices in 4 economic areas, and we are interested in the state of legislation regarding tools based on artificial intelligence in each of them. In all areas, the legislation mainly focuses on ensuring national security, preventing abuse or fraud using AI and maintaining privacy. Analysing the reports [8], many legislative initiatives are planned for 2024 worldwide. Coding support is either omitted from these efforts entirely or merely classified as low-risk.

// India

India, as one of the fastest-growing economies in recent years, is recognising the opportunities arising from the use of AI for economic transformation. In June 2018, the “National Strategy for Artificial Intelligence” [9] was released, describing guidelines for the development of artificial intelligence. Two reports were issued in 2021: “Part 1: Principles for Responsible AI” [10] in February and “Part 2: Operationalizing Principles for Responsible AI” [11] in August, which described the actions necessary to be taken by the government, private sector, and research centres to ensure ethical use of AI.

In August 2023, the “Digital Personal Data Protection Act” [12] was issued, relating to the processing of private digital data. AI-based tools should respect its provisions.

The Indian government is working on a draft regulation relating to tools using artificial intelligence. The document will be published in mid-2024.

// EU

In 2021, the European Parliament developed the “AI Act” [13], which introduced the division of AI systems depending on the risk arising from their use, to ensure security, transparency, and non-discrimination. On March 13, 2024, the European Parliament passed regulations on AI standards by an overwhelming majority [4]. It prohibits certain uses of artificial intelligence that threaten citizens' rights.

These include:

- biometric categorisation systems that use sensitive features and untargeted downloads of facial images from the Internet or CCTV footage to create facial recognition databases;
- emotion recognition systems in the workplace and educational institutions;
- point classification of citizens;
- crime forecasting solely based on profiling a person or assessing his or her characteristics;
- manipulating human behaviour;
- exploiting human weaknesses.

[8] https://iapp.org/resources/article/global-ai-legislation-tracker/
[9] https://indiaai.gov.in/research-reports/national-strategy-for-artificial-intelligence/
[10] https://indiaai.gov.in/research-reports/responsible-ai-part-1-principles-for-responsible-ai
[11] https://indiaai.gov.in/research-reports/responsible-ai-part-2-operationalizing-principles-for-responsible-ai
[12] https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
[13] https://artificialintelligenceact.eu/

The EU may impose financial penalties for failure to comply with the guidelines. The new law also includes a requirement for the transparency of publicly available artificial intelligence models and the need to comply with copyright laws. Such systems will need to provide a list of the information sources used to train their models. In addition, an obligation is introduced to mark inauthentic or manipulated images, audio, or video content.

// UK

In March 2023, the UK government published a whitepaper [14] on artificial intelligence regulation, focusing on a pro-innovation approach while ensuring safety and accountability. It outlines five cross-sectoral principles for regulators to follow and proposes a central function to enhance regulatory consistency and address gaps. The British government mentions in its publications the issue of copyright protection of data used for training the model. Recommendations have been issued for regulators to update their AI strategies by April 30, 2024.

// US

The United States is a pioneer in the field of AI. Government structures are aware of this and do not want to block further progress through legislation so that their leadership position in AI is maintained. The President of the United States signed an “Executive Order” [15] on October 30, 2023, which focused on mitigating the risks arising from the use of AI by, among other things: requiring developers of the most powerful AI tools to share critical information with the government before making the product public; the development of tools to validate AI systems by the National Institute of Standards and Technology (NIST); and providing tools to protect American citizens from fraud resulting from the use of AI-generated materials.

Responsible business in the age of AI

Creating laws at the state level is an inherently slower process than technological development. It is important to prepare a clear policy for the use of AI tools especially for a company operating in various economic areas, each with different legislation. This document should take into account local regulations to consistently define rules across all office locations. It should support building awareness of the threats resulting from the use of AI in the company.

Maintaining security and privacy standards is possible by defining rules for, among others, the following areas:

- Protection of confidential data
  - full prohibition on sharing confidential data or requiring written authorisation to do so
- Access control
  - prohibition of access to tools to unauthorised persons or external parties
- Transparency
  - informing your supervisor, contractor or co-workers about how generative AI tools are used
- IP rights and proprietary information
  - making employees aware of the implications regarding generative AI and copyright
  - sharing of methods for minimising IP rights violation risk to the company
- Training and education
  - providing employees with information on the threats resulting from the use of AI
  - presenting good practice in the use of AI
- Incident reporting
  - describing a clear process for reporting incidents
- Legal compliance
  - list of standards with which tools used in the company must comply (e.g. GDPR) o determining what AI can be used for within the company and what types of products it can be used to develop

[14] https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
[15] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

// Summary

AI is revolutionising the world economy, the digital market and software development. The use of generative AI tools can pose risks related to intellectual property infringement, especially when it comes to copyright claims regarding AI-generated content. Companies can take measures to prevent such infringements and minimise associated risks by implementing policies that address issues such as the protection of confidential data, access control, transparency, IP rights, training and education, incident reporting, and legal compliance.

Additionally, legislation related to AI is emerging in various economic areas, with the EU recently passing regulations on AI standards and other regions such as India and the UK working on draft regulations. Companies need to stay informed about these developments and ensure compliance with applicable laws when using AI tools

Partner with Consult Red on your next project

Are you looking for an innovative software development partner who has harnessed the benefits of AI-enabled development tools, while considering best practices in terms of security and privacy? Contact Consult Red.