▯▯ The Future of AI Privacy Risks: Balancing Technology and Rights

Maria Cattini | 05/05/2025 | Cybersecurity

AI tools like ChatGPT, Midjourney, and Gemini are becoming part of our everyday lives. We use them to generate text, images, ideas—and often, without realizing it, we feed them with **personal or even confidential information**.

But… do you know what happens to your data once it's uploaded?

▯▯ Where Do Your Data Go?

Every time you enter a prompt, upload an image, or speak into a voice assistant, you're handing over data. But:

- **Who has access** to that data?
- **Where is it stored?**
- Could it be used to **train future AI models**?

These are not hypothetical questions.

In 2023, a Japanese tech company **banned employees from using ChatGPT** after discovering that business-sensitive information was being processed without guarantees of confidentiality.

⚠ What Are the Risks?

Modern AI systems are trained on vast amounts of data—and sometimes, user input becomes part of that data.

Here’s what can go wrong:

- **Data leaks** via cloud storage or third-party access
- **Loss of control** over how your content is used
- **Lack of transparency** on how your data is processed, especially outside the EU

Add to that the viral spread of deepfake images (remember the Pope in a Moncler puffer?), and it's easy to see why **AI privacy is no longer just a geek issue**—it affects everyone.

□ How to Protect Your Data When Using AI Tools

Here are three simple steps to boost your digital safety:

1. Check Privacy Settings

Most advanced AI tools now offer options to disable conversation history or data usage. For example:

> In ChatGPT, go to Settings → Data Controls → Turn off “Chat history & training”.

2. Never Share Sensitive Information

Avoid entering:

- Real names, addresses, or ID numbers
- Company secrets or confidential documents
- Anything you wouldn't want to see reused elsewhere

3. Know Your Rights with the EU AI Act

Since March 2024, the **AI Act** requires AI platforms to:

- Be clear about how data is collected and used
- Allow users to opt out of training
- Guarantee transparency and accountability

□□ The Big Picture: AI Is Powerful—But Not Infallible

AI can write articles, design logos, plan your trips. But it also collects, stores, and analyzes your input.

The more we use it, the more we need to:

- **Stay informed**
- **Use AI mindfully**
- **Push for stronger data protection policies**

Want to Dive Deeper?
Join our Telegram channel **for real-time tips on AI, OSINT, and digital security**
Subscribe to the newsletter **to get updates like this every week**