07.02.2023

New content on AI and ChatGPTChat robots, image generators and other AI systems have been unleashed on internet users from IT research labs for several weeks. A reason to take a closer look at data protection in artificial intelligence.©

DALL-E (robots, network, calculating, text)Write the essay about Vincent van Gogh with just a few clicks instead of laboriously collecting different sources and constructing beautiful sentences, this is promised by software that is currently very popular with schoolchildren and students delighted. At this year's Safer Internet Day (SID), the State Commissioner for Data Protection and Freedom of Information of Rhineland-Palatinate takes a look at the topic of artificial intelligence (AI). For a few weeks now, the "ChatGPT" speech robot has arrived in schools, which can create texts that seem to have been written by the student's hand on all sorts of lesson topics in seconds. This is just one example of how AI systems can be found more and more in digital applications in our everyday lives. Data protectionists have been following developments in the field of AI for several years and in particular point out the dangers that the systems can pose. "AI systems, whether in language assistants, research or security agencies, can perform human tasks in a fraction of the time and are therefore becoming more widespread as support. The problem is that in many of the systems, the algorithm that makes the decisions is a black box. Dieter Kugelman. "Whoever develops and controls the algorithm determines the results. This can quickly lead to tendentious or incorrect results, political influence or racial discrimination. Transparency of the algorithms and the possibility of having the systems checked by independent third parties are therefore the be-all and end-all before introducing corresponding AI systems, for example in the area of government action. already defined seven requirements for AI systems in the Hambach Declaration on Artificial Intelligence in 2019, which are intended to help prevent misuse. A closer look at the results of the chat robots or image generators shows that the "intelligence" of the systems still has limits. The texts are often written perfectly in terms of language, but the content does not go into too much detail or they are simply wrong. The image generators also fail when creating the - otherwise photorealistic - images, even with details such as eyes, fingers or objects such as glasses. In order to deliver real perfection here, the systems simply lack even more human data. This is one of the main reasons why the login for some systems has been open to everyone since autumn 2022. In the first few weeks, millions of users flocked to the platforms, some of which can only be used when they are logged in with an account, and feed the algorithm with data, including their cell phone number, with each of their entries. An immense, valid test group that the

operating companies and financiers behind the programs could never have bought with their own funds. And this despite, for example, the announced investment of 10 billion US dollars by the US group Microsoft in ChatGPT. Only the supposedly playful chat activity of many millions of users with the robot creates the rapidly growing database that can be exploited to improve the systems. For teachers, it is now a good opportunity to get into the topic and to engage with the students in a constructive and critical way with the programs," says Prof. Kugelmann provide further information in the coming months, which is intended to give pupils a better insight into the world of AI and the protection of their personal data in Italy return