The Right Not to Be Subjected to AI Profiling Based on Publicly Available Data—Privacy and the Exceptionalism of AI Profiling, Thomas Ploug

Keywords: Mental health profiling/ Artificial intelligence/ Social media data/ Autonomy/ Depression

Analyzing social media with AI to predict health conditions holds immense potential. Studies have shown that using machine learning models on Instagram photos can identify depressed users with greater accuracy than unassisted general practitioners. Predictive factors for depression on social networks include the brightness and colors of photos, the number of comments and likes. Bluer, darker, and grayer photos are associated with depression, as well as those receiving more comments but fewer likes. On Twitter, the use of negative words, fewer positive words, and a higher word count are associated with depression. These models have also shown promising results in predicting other mental disorders and risks, such as anxiety, bipolar disorder, borderline personality disorder, schizophrenia, autism, suicide risk, and anorexia. This has sparked a debate on AI regulation due to its increased predictive potential and widespread use in different sectors. The article discusses the benefits and risks of mental health profiling from social media data, highlighting privacy concerns related to using public data for sensitive predictions. It proposes establishing a specific legal right not to be subjected to AI profiling based on public data without explicit and informed consent. This right allows for refusal of interference in AI profiling using sensitive online and public personal data. It can be waived by informed consent and may be restricted under exceptional conditions. The article argues for the need for a four-step sui generis right. It explains that personal data protection prevents social control and stigma, mentions the unique threat of AI profiling, underscores the importance of protecting public discourse on social media, and concludes that current European legislation is insufficient to ensure a right not to be profiled by AI. Three examples of mental health profiling by AI are presented, covering various contexts such as a situation among friends and a case involving a politician. Furthermore, the article advances two autonomy-based arguments to justify the right to privacy: the social pressure argument, which defends individuals' right to protect themselves against undesirable social influence, and the open future argument, which emphasizes that disclosing certain personal data can harm individuals' future opportunities, contradicting their interests. The stigma argument highlights the potential harms of stigma related to accessing certain personal data. In summary, here are four main reasons for protecting individuals against AI profiling. AI profiling stands out for its ability to predict individuals' future behavior, thereby exposing them to attempts at social control. Moreover, this increased accuracy can increase the risk of stigmatization by reinforcing beliefs in the predictability of human behavior. The AI-based approach exposes individuals to the collection and use of their personal data for profiling purposes, making them more vulnerable. Additionally, this can also have consequences for individuals' loved ones, exposing them to the same risks of social control and stigma. In summary, these arguments support the necessity of protecting everyone's right not to be profiled by AI, especially when based on publicly accessible personal data. The article acknowledges the social and democratic benefits of online data sharing but also highlights the risks to individual autonomy, well-being, and democracy associated with AI profiling. In conclusion, individuals should have the right to refuse AI profiling based on their personal data to protect their autonomy and well-being. This article examines whether the GDPR already incorporates such a right. Although the GDPR does not explicitly provide for this right, it could indirectly guarantee it by prohibiting certain types of mental health-related profiling. Two approaches are conceivable for verifying whether the GDPR implies such a right: analyzing the GDPR's processing principles or assessing the scope of these principles and any permitted restrictions. The three cases studied involve different levels of protection under the GDPR. For friends, profiling seems to be considered a personal and domestic activity, thus escaping the GDPR. For public officials, Member States can tailor the GDPR principles to allow profiling based on public interests such as social security. Additionally, prime ministerial candidates benefit from exemptions for journalistic or public interest activities, thus providing some flexibility regarding profiling. The article argues for the necessity of an explicit right not to be profiled by AI to avoid risks of harm. Such a right would simplify regulation and strengthen control over AI use. This article questions the necessity and limits of the right and highlights the importance of informed consent in protecting individuals.