

# **Análise do caso de *Clearview AI* e Matthias Marx**

*Trabalho elaborado como parte 2 no âmbito da  
Unidade Curricular de Segurança, Ética e  
Privacidade do 2º ano da Licenciatura em Ciência de  
Dados*

**Plancha; 105289**

*ISCTE-IUL*

27 de dezembro de 2022, Versão 1.0.1

## *ClearviewAI*

Em 2020, Matthias Marx apresentou uma queixa dentro do Regulamento Geral sobre a Proteção de Dados (RGPD) contra a Clearview AI, uma empresa americana especializada em reconhecimento facial (RF), por ter guardado e processado as suas fotos públicas sem o seu conhecimento e consentimento (Meaker, 2022). Embora pareça intuitivo que Marx esteja no seu direito de reclamar, devido à quebra de vários artigos do RGPD, incluindo os artigos 13 e 14, questões morais sobre o caso e o próprio processo de recolha e uso dos dados executado pela empresa podem ser levantadas.

Neste ensaio, estas questões vão ser analisadas usando o método de Bynum (Bynum & Rogerson, 2003), de forma a entender melhor o caso e a sua relevância, bem como a sua importância para o futuro da privacidade e proteção de dados, em termos de ética digital e de responsabilidade social.

## *Análise do caso*

### **Ponto de vista ético**

Este caso possivelmente envolve questões éticas em vários valores éticos, incluindo potencialmente a privacidade, segurança, propriedade intelectual e consentimento de Marx, a liberdade de expressão e informação da empresa, e da privacidade e segurança pública e privada dos cidadãos.

### **Participantes**

O caso em questão envolve os seguintes participantes (Plancha, 2022):

*Clearview AI*: A empresa que desenvolveu a sua ferramenta de RF, criando perfis biométricos de pessoas a partir das suas fotos publicadas em redes sociais, blogs, ou qualquer outro *site* que a ferramenta tenha acesso a, de forma a combater o crime, sem o consentimento e conhecimento dos indivíduos;

Matthias Marx: O indivíduo que apresentou a queixa, e que sentiu que a sua privacidade tinha sido quebrada após um Pedido de Acesso dos Dados do Titular (PADT) à *Clearview AI*, revelando as suas fotos associados ao seu nome, apenas com reconhecimento da sua face; Marx também não garantiu que as suas fotos não tenham sido publicadas por terceiros ou por ele mesmo, tornando tais fotografias acessíveis a qualquer pessoa (ou máquina) com acesso à internet;

Agentes não humanos: As ferramentas que levaram à queixa foram o *web crawler*, a base de dados e o sistema de RF. De forma a facilitar a descrição, cada um deles vai ter o nome de A\_WC, A\_BD e A\_RF, respectivamente.

Engenheiros do sistema: Os engenheiros que criaram a ferramenta de RF e usaram técnicas de *web crawling* para recolher e guardar as fotos públicas de indivíduos, sem o seu consentimento, podem potencialmente ter quebrado código de conduta e ética profissional, na construção do programa;

Reguladora alemã: A autoridade que processou a queixa de Marx sobre a quebra do RGPD.

### **Questões éticas e problemas**

A\_WC guardou as imagens de Marx sem o seu consentimento, de forma a serem identificadas pela A\_RF. Quem é o responsável aqui? A quebra de privacidade e do RGPD de indivíduos da União Europeia foi intencional ou uma consequência não prevista? Foram essas quebras necessárias para a segurança pública? As quebras foram feitas pelo processo de qual ferramenta/cominação de ferramentas: A\_WC, A\_BD ou A\_RF? Quem é responsável por estas quebras: o CEO, os engenheiros ou Marx? Se a quebra de privacidade fosse não intencional, quem são os responsáveis? Foi apenas um acidente ou uma falha de segurança? A empresa está a recolher fotos de indivíduos fora dos Estados Unidos. Há alguma forma de impedir este resultado? Deve a empresa americana importar-se com esses indivíduos, sendo que esses não são o seu foco? E se a ferramenta apenas for usada no país, deve ela preocupar-se com a identificação de indivíduos fora dele? Se a ferramenta for suficientemente correta no seu reconhecimento e nos seus perfis, há possibilidade dos dados de Marx e outros serem expostos e usados de forma imoral ou ilegal? A própria ferramenta seria ilegal se fosse usada na Europa? Se os agentes fossem roubados por terceiros, seria possível que a segurança e privacidade de Marx estivessem em risco? Este caso podia ter sido evitado de alguma forma?

## **Análise sistemática**

De seguida vai ser feita uma análise do caso de acordo com diferentes sistemas de análise de moralidade, tendo em conta os direitos e deveres de cada um dos participantes onde questões éticas foram levantadas:

### **Utilitarismo** De acordo com Mill (1861),

A crença que aceita como fundamento da moralidade a Utilidade, ou o Princípio da Maior Felicidade, sustenta que ações são corretas na medida em que tendem a promover a felicidade [total], e erradas na medida em que tendem a produzir o contrário da felicidade [total].

Em utilitarismo clássico, consegue-se ser argumentado que a quebra de privacidade pode ser considerado moralmente aceitável para uma segurança pública mais ampla, e RF seria uma forma de melhorá-la. No entanto, pode ser argumentado também que uma potencial quebra de informação para terceiros sem as melhores intenções pode levar um utilitarista a negar estas situações positivas. Pelo mesmo facto, ninguém garante que esta empresa não tenha tais intenções.

Consegue ser também argumentado que a execução de recolha dos dados não foi a que promove maior felicidade, sendo que a falta de conhecimento e consentimento da vítima levou a uma infelicidade maior. Técnicas, ou métodos de recolha de biometria alternativos conseguem quebrar a privacidade de forma mais aceitável, com a mesma consequência, assim promovendo maior felicidade. Como por exemplo, a companhia podia ter coletado apenas fotografias usadas de forma consentida, como fotos de perfil de redes sociais, ou fotos de documentos de identificação, ou ter apenas recolhido impressões digitais.

Em outras teorias de utilitarismo, como o utilitarismo de Popper (1966):

[...] um humano a sofrer faz um apelo moral direto, especificamente, o apelo por ajuda, enquanto que não há apelo semelhante para aumentar a felicidade de um homem que esteja bem.

Neste caso, como a vítima sofreu devido à quebra de privacidade, e a potencial violação de dados pode levar a uma infelicidade maior, pode ser argumentado que a quebra de privacidade foi moralmente errada.

### **Deontologia** Kant, filósofo famoso pela sua teoria deontológica, concluiu que (1785):

O bem preeminente que chamamos moral não pode, portanto, consistir em nada mais do que a concepção da lei em si, o que certamente só é possível num ser racional, na medida em que essa concepção, e não o efeito esperado, determina a vontade.

Para Kant, uma ação é moralmente correta quando o agente atua no ser dever, e a consequência da ação esperada é irrelevante para o valor moral. Neste caso, consegue-se argumentar que a empresa privada tem o dever de não quebrar a privacidade da vítima, e portanto agiu de forma moralmente incorreta. Se o objetivo for a segurança pública, então tal empresa deve fazê-lo de forma a não quebrar o seu dever à privacidade de clientes e cidadãos.

Da mesma forma, o Código de Ética de Engenharia de *Software* (Gotterbarn et al., 1997) declara alguns princípios que os engenheiros e a organização não atuaram de acordo, como:

- 1.10 "Trabalhe para desenvolver software [...] que respeitam a privacidade daqueles que serão submetidos a esse software";
- 1.13 "Trabalhe para identificar, definir e remediar problemas éticos, económicos, culturais, legais e ambientais relacionado com qualquer projeto";
- 2.01 "Divulgue às pessoas ou autoridades apropriadas de qualquer perigo real ou potencial para o usuário, um terceiro, ou meio ambiente, que ele razoalmente acredite estar associado ao software ou documentos relacionados pelos quais eles são responsáveis, ou apenas sabem sobre"

## **RGPD**

O Regulamento Geral de Proteção de Dados (RGPD) é um regulamento europeu que define regras para a proteção de dados pessoais de cidadãos europeus. Este regulamento foi criado para proteger os direitos dos cidadãos europeus, e para garantir que as empresas que lidam com dados pessoais sigam regras específicas para proteger os dados pessoais.

O caso como descrito consegue quebrar vários artigos do RGPD, como o Artigo 6.º, que define a licitude do tratamento. Nele se descreve que o tratamento só é lícito se O titular consentir, ou for necessário para a execução de: um contrato, obrigação jurídica, defesa do titular dos dados, exercício de funções de interesse público, ou para fins de interesses legítimos, excepto se prevalecerem os interesses do titular. Neste caso, apenas pode ser argumentado que o tratamento é lícito se conseguir-se provar a necessidade do interesse público, sendo que todos os outros pontos claramente não são argumentáveis. No entanto, para o tratamento ser lícito, o artigo expõe também que o contexto em que os dados foram recolhidos deve ser considerado, e que têm que existir salvaguardas adequadas, como a cifragem ou a pseudonimização, o que consegue ser argumentado que o caso não cumpre.

Da mesma forma, o Artigo 9.º declara que "é proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, [...], bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, [...]", sendo que nenhuma das exceções se aplicam ao caso.

## Conclusões e futuro

O caso descrito é um exemplo de RF feito de forma moralmente questionável, e não cumpre com os regulamentos europeus de proteção de dados. *Clearview AI* deve ter em conta a moralidade e legalidade das suas ferramentas e dos seus agentes, mesmo que apenas disponibilize o serviço fora dos estados membros da União Europeia. Outras empresas, companhias e governos devem também ter em conta a moralidade de técnicas de reconhecimento facial e empregá-las de forma segura e legal, de forma a não violar os direitos dos cidadãos, nacional e internacionalmente. Se isso não for possível nesta técnica de biometria, então dificilmente será o suporte para tal.

## Referências

- Bynum, T., & Rogerson, S. (2003). *Computer Ethics and Professional Responsibility*. Wiley.
- Gotterbarn, D., Miller, K., & Rogerson, S. (1997). Software engineering code of ethics. *Communications of the ACM*, 40(11), 110–118. <https://doi.org/10.1145/265684.265699>
- Kant, I. (1785). *Groundwork for the Metaphysics of Morals* (T. K. Abbott, Trad.). Wikisource. [https://en.wikisource.org/wiki/Groundwork\\_of\\_the\\_Metaphysics\\_of\\_Morals](https://en.wikisource.org/wiki/Groundwork_of_the_Metaphysics_of_Morals)
- Meaker, M. (2022). Clearview Stole My Face and the EU Can't Do Anything About It. *WIRED*. <https://www.wired.com/story/clearview-face-search-engine-gdpr/>
- Mill, J. S. (1861). *Utilitarianism* (W. contributors, Trad.). Wikisource. <https://en.wikisource.org/wiki/Utilitarianism>
- Plancha. (2022). *Clearview AI e Matthias Marx*. <https://github.com/notPlancha/projeto-sep/raw/master/first/first.pdf>
- Popper, K. R. (1966). *The Open Society and Its Enemies. Vol. 1*. London, Routledge; K. Paul.