Parte I

1 . Segundo Moor, os computadores são logicamente maleáveis, uma vez que podem ser manipulados para fazer qualquer atividade que possa ser caracterizada em termos de entradas, saídas e operações lógicas.

A maleabilidade lógica tem um grande impacto na ética computacional porque permite o surgimento de novos desafios éticos à medida que a tecnologia computacional vai evoluindo. Existem vários exemplos destes impactos tais como:

A criação de "vazios de políticas", que consistem na inexistência de políticas para determinadas situações, que necessitam que sejam criadas novas políticas para lidar com os problemas inéditos que vão aparecendo.

A expansão dos desafios éticos tradicionais, uma vez que a flexibilidade dos computadores amplia dilemas éticos já existentes, existe por exemplo o caso da privacidade, em que a vigilância em massa e outros aspetos da tecnologia exigem políticas mais detalhadas.

A ambiguidade moral das tecnologias computacionais, uma vez que por causa da maleabilidade lógica dos computadores, eles podem ser usados para fins positivos ou negativos. Esta ambiguidade necessita que os profissionais de informática considerem o impacto social do seu trabalho.

A responsabilidade social, uma vez que os impactos sociais das tecnologias podem ser imprevisíveis e os profissionais de informática devem adotar princípios de ética sólidos ao desenhar novos sistemas que podem afetar a vida das pessoas.

Concluindo, a maleabilidade lógica é uma característica que torna os computadores poderosos e adaptáveis mas também desafia a ética computacional ao criar dilemas inéditos e complexos.

2 . Os códigos de ética mais aplicáveis no contexto de engenharia informática são o ACM (Association for Computing Machinery) Code of Ethics and Professional Conduct, o IEEE Code of Ethics e o SECEPP (Software Engineering Code of Ethics and Professional Practice).

O ACM define princípios que guiam os profissionais de informática, enfatizando responsabilidades como contribuir para o bem estar da sociedade, evitar causar danos através da tecnologia, garantir honestidade e transparência sobre as capacidades e limitações dos programas e respeitar a privacidade e os direitos dos utilizadores. Assim, o ACM garante que os engenheiros informáticos desenvolvam sistemas seguros e éticos, minimizando riscos e promovendo a confiança da tecnologia.

O IEEE foca na integridade profissional e no impacto social da tecnologia, com princípios como priorizar a segurança e o bem estar público, reportar práticas desonestas ou anti-éticas e rejeitar subornos e conflitos de interesse. O IEEE incentiva a transparência e a responsabilidade, garantindo que os engenheiros tomem decisões que protejam os

interesses do público.

O SECEPP foi desenvolvido em parceria pela ACM e IEEE, foca especificamente na ética da engenharia de software e inclui oito princípios: proteger o interesse do público, atuar no melhor interesse dos clientes, garantir qualidade e segurança no desenvolvimento de software, manter independência e responsabilidade nas decisões, incentivar praticas éticas dentro da equipa, promover a reputação da engenharia de software, respeitar e colaborar com outros profissionais e melhorar continuamente as competências profissionais.

Assim, estes códigos de ética direcionam os engenheiros a equilibrar os interesses técnicos e éticos, assegurando que os produtos de software respeitam os direitos fundamentais como privacidade e acessibilidade.

3 . Os engenheiros enfrentam desafios éticos e profissionais ao equilibrar as suas responsabilidades perante a sociedade, o empregador e a família. Como profissionais devem garantir que o seu trabalho beneficie a sociedade, cumpra os interesses do empregador e ao mesmo tempo permita um equilíbrio saudável com a vida pessoal. Para conciliar estas responsabilidades é necessário adotar estratégias nestas três áreas.

Perante a sociedade, o engenheiro deve garantir que os seus produtos e serviços respeitam os direitos dos cidadãos e promovam o bem-estar social. Para atingir este fim devem guiar-se pelos códigos de ética que os orienta a desenvolver software seguro, transparente e responsável. Como exemplo, um engenheiro que trabalha no desenvolvimento de um sistema de vigilância deve garantir que ele respeite as leis da privacidade e não seja usado para fins abusivos.

Perante o empregador, o engenheiro tem o dever de agir no melhor interesse do seu empregador, cumprindo prazos, mantendo a confidencialidade das informações e garantindo a eficiência dos projetos. No entanto, a lealdade ao empregador não se deve sobrepor à ética profissional. Por exemplo, se o seu empregador pedir que um software seja lançado sem testes de segurança adequados, o engenheiro deve alertar sobre os riscos e sugerir alternativas para mitigar possíveis problemas.

Perante a família, o engenheiro deve garantir um equilíbrio saudável entre a vida profissional e a pessoal, gerindo o tempo de forma eficiente e evitando excessos de trabalho que comprometam a sua saúde mental e bem-estar familiar. Algumas empresas adotam políticas de flexibilidade no trabalho e de incentivo ao bem-estar dos funcionários, permitindo que cumpram as suas responsabilidades familiares sem comprometer a produtividade. Por exemplo, um engenheiro que trabalhe longas sem pausas pode comprometer a sua vida familiar e a própria eficiência no trabalho. Adotar uma rotina equilibrada e definir limites de trabalho são estratégias essenciais para manter a qualidade de vida.

Concluindo, estas são as estratégias que um engenheiro deve aplicar para conciliar as suas responsabilidades garantindo um desempenho responsável e sustentável na profissão.

Parte II

4.1 O caso envolve João, um engenheiro informático que trabalha numa empresa de tecnologia especializada em software de monitorização e vigilância. A empresa recebeu um contrato de um governo autoritário para desenvolver um sistema de vigilância avançado, que inclui reconhecimento facial, rastreamento de redes sociais e localização em tempo real.

Durante o desenvolvimento, João percebe que esse sistema pode ser usado para violar direitos humanos, permitindo a opressão de dissidentes políticos e minorias. Ele enfrenta um dilema ético: deve continuar a trabalhar no seu projeto, cumprindo as suas obrigações profissionais, ou denunciar os riscos e possivelmente colocar a sua carreira em perigo?

4.2 Na análise deste caso, o prejuízo é o uso indevido deste sistema que pode ter consequenciais como a opressão política, prisões arbitrarias e perseguições a grupos vulneráveis. O João pode sofrer consequências profissionais, e até legais, se decidir denunciar o caso. A empresa pode enfrentar sanções internacionais se for descoberta desenvolvendo tecnologia para regimes opressores.

A Justeza do caso é definida pelos seguintes factos: O projeto pode ser apresentado como ferramenta de segurança nacional, mas a sua implementação viola a liberdade individual e a privacidade. Se o João permanecer em silêncio, ele estará indiretamente a contribuir para possíveis abusos de direitos humanos.

Em relação ao preconceito, o sistema pode ser utilizado para discriminar minorias e perseguir grupos políticos, intensificando injustiças sociais.

E por fim, a razoabilidade: Embora a empresa tenha um contrato legalmente válido, é eticamente irresponsável desenvolver tecnologia que pode ser usada para fins opressivos. O João precisa decidir se a sua lealdade deve ser a empresa, ou aos princípios de ética e direitos humanos.

4.3 Este caso levanta questões éticas complexas, relacionadas ao uso da tecnologia para vigilância governamental. Essas questões são:

A violação de direitos humanos, uma vez que o sistema pode ser utilizado para controlar e punir cidadãos inocentes, comprometendo a liberdade e a segurança individual.

A responsabilidade profissional e moral já que o João como engenheiro, deve seguir um código de ética que priorize o bem-estar social e evite desenvolver ferramentas prejudiciais.

O dilema da denuncia vs segurança pessoal e profissional, porque se o João denunciar o caso pode enfrentar retaliações da empresa ou do governo. No entanto, se permanecer em silêncio contribuirá para um sistema que poderá ser usado de forma anti-ética.

O uso ético da inteligência artificial e da vigilância, uma vez que as tecnologias de

monitorização devem respeitar a privacidade e os direitos fundamentais da população.

4 . 4 Este caso pode ser analisado sobre os princípios do Software Engineering Code of Ethics and Professional Practice (SECEPP), nomeadamente, os princípios um, três e seis.

O princípio um é definido pelo público, em que os engenheiros devem garantir que seus produtos sejam usados para o bem da sociedade.

O princípio três é definido pelo produto, uma vez que o software desenvolvido deve ser seguro e não prejudicar os utilizadores.

E por fim, o princípio seis que é definido pela profissão porque a engenharia de software deve manter altos padrões éticos, evitando projetos que possam violar direitos humanos.

4.5 Depois de analisar este caso, as minhas conclusões são que o sistema de vigilância tem um potencial claro de abuso e pode comprometer direitos humanos fundamentais. Ao mesmo tempo, o João enfrenta um dilema ético real, pois a sua participação pode ter consequências sociais graves, mas a sua saída do projeto pode prejudicar a sua carreira. A empresa tem responsabilidade ética sobre os produtos que desenvolve, devendo garantir que a tecnologia não seja utilizada para opressão política. A decisão do João pode depender de alternativas seguras, como a denúncia interna, alertar uma organização de direitos humanos ou procurar apoio jurídico.

Concluindo, a ética computacional exige que engenheiros tomem decisões conscientes e avaliem se eu o trabalho contribui para um futuro justo ou perpetua praticas opressivas.