3 de dezembro de 2023

Dado que os utilizadores, n˜ao apenas consumidores, mas tamb´em participantes na fase de teste, possuem o direito `a privacidade e constituem parte integrante da comunidade, torna-se imperativo tomar decis˜oes que favore¸cam todas as partes envolvidas, respeitando integralmente a privacidade de cada indiv´ıduo e resolvendo eventuais conflitos.

Quando apresentamos aos utilizadores a op¸c˜ao de consentir ou n˜ao com o compartilhamento de seus dados, ´e observado que a op¸c˜ao de consentir, n˜ao surpreendentemente, atrai mais aten¸c˜ao, enquanto a op¸c˜ao de recusar, muitas vezes, requer mais cliques e, em diversas situa¸c˜oes, limita a funcionalidade do produto. No entanto, podemos tomar a iniciativa de estabelecer a n˜ao partilha de dados como a op¸c˜ao padr˜ao, apresentando ambas as escolhas de maneira clara em um pop-up. Ap´os o treino do modelo, podemos limitar a requisic˜ao de dados apenas a situa¸c˜oes que se desviem do ordin´ario.

Aqueles que optarem por compartilhar dados devem ser apresentados com um mapa completo de todos os processos pelos quais seus dados ser˜ao submetidos, proporcionando uma vis˜ao transparente desse processamento. Isso se torna ainda mais crucial para produtos em fase de teste nos quais o treino do modelo de inteligˆencia artificial ´e necess´ario. Nesse contexto, a coleta de dados ´e obrigat´oria, mas os utilizadores n˜ao apenas est˜ao cientes do caminho percorrido pelos seus dados, como tamb´em recebem algo em troca dessa partilha.

Adicionalmente, para garantir uma camada extra de privacidade para todos os utilizadores, po- demos implementar localmente modelos de inteligˆencia artificial capazes de identificar humanos e animais, bem como de desfocar as faces correspondentes. Existem modelos open-source, como o [Mo-](https://arxiv.org/abs/1704.04861) [bileNet,](https://arxiv.org/abs/1704.04861) [YOLO](https://arxiv.org/abs/1506.02640) (You Only Look Once), dois deep neural networks leves para identifica¸c˜ao de objetos, e o [Blurry Faces,](https://github.com/asmaamirkhan/BlurryFaces) que, como o pr´oprio nome indica, tem a capacidade de desfocar as faces das pessoas. Se a transmiss˜ao de dados for necess´aria e o utilizador optar por fazˆe-lo, ´e poss´ıvel empregar pro- tocolos de transmiss˜ao que oferecem maior privacidade, como o [SFTP](https://www.ssh.com/academy/ssh/sftp-ssh-file-transfer-protocol) (Secure File Transfer Protocol),

prevenindo assim vazamentos de dados.

Al´em disso, ap´os a fase de teste de produtos direcionados aos utilizadores chegar ao fim, todos os dados capturados posteriormente pelo produto podem ser processados localmente. Isso justifica-se pelo facto de que a utiliza¸c˜ao do modelo necessitar significativamente menos poder computacional em compara¸c˜ao com o seu treino.

Dado que os utilizadores (n˜ao s´o consumidores, mas tamb´em aqueles que participam na fase de teste) tˆem o direito `a privacidade e que estes fazem parte da comunidade, precisamos de tomar decis˜oes que tentem favorecer todas as partes respeitando a privacidade de todos, ou seja, resolvendo os conflitos.

Quando ´e apresentado ao utilizador a quest˜ao de optar ou n˜ao por partilhar os seus dados, a op¸c˜ao que mais chama a aten¸c˜ao ´e, sem surpresas, a de concordar sendo que para rejeitar n˜ao s´o requer mais cliques como tamb´em muitas das vezes limita a funcionalidade do produto. No entanto, podemos tomar a iniciativa de tornar a n˜ao partilha de dados a op¸c˜ao por defeito, mostrando ambas as op¸c˜oes de forma clara no pop-up (sendo que ap´os o treino do modelo, podemos apenas requerer dados de momentos que possam ser fora do ordin´ario).

Aqueles que optem por partilhar dados devem ser apresentados com um mapa de todos os processos pelos quais os seus dados v˜ao passar, dando ao utilizador uma vis˜ao transparente desse processamento. Isto ´e ainda mais importante para produtos teste nos quais ´e ainda necess´ario o treino do modelo de inteligˆencia artificial, neste caso torna-se obrigat´orio a recolha de dados, mas os utilizadores n˜ao s´o sabem por onde v˜ao passar os seus dados, como tamb´em ´e mencionado no texto, recebem algo em troca disso.

Para adicionar uma outra camada de privacidade para todos os utilizadores, podemos tamb´em implementar localmente outros modelos de inteligˆencia artificial para identificar humanos e animais e desfocar a cara dos mesmos. Existem modelos open-source que foram implementados e treinador com o objetivo de poderem ser corridos localmente com um processador menos potente, como exemplo, temos MobileNet, Yolo, dois lightweight deep neural networks para identifica¸c˜ao de objetos, e Blurry Faces que tal como o nome indica desfoca a cara de pessoas.

Se for necess´ario a transmiss˜ao de dados e o utilizar optar por assim o fazer, existem protocolos de transmiss˜ao que oferecem uma maior privacidade, como SFTP, prevenindo data leaks.

Adicionalmente, para produtos direcionado a utilizadores, como fase de teste se apresenta finda, todos os dados capturados pelo produtos podem ser processados localmente, dado que a utiliza¸c˜ao do modelo requer muito menos poder computacional em rela¸c˜ao ao treino do mesmo.