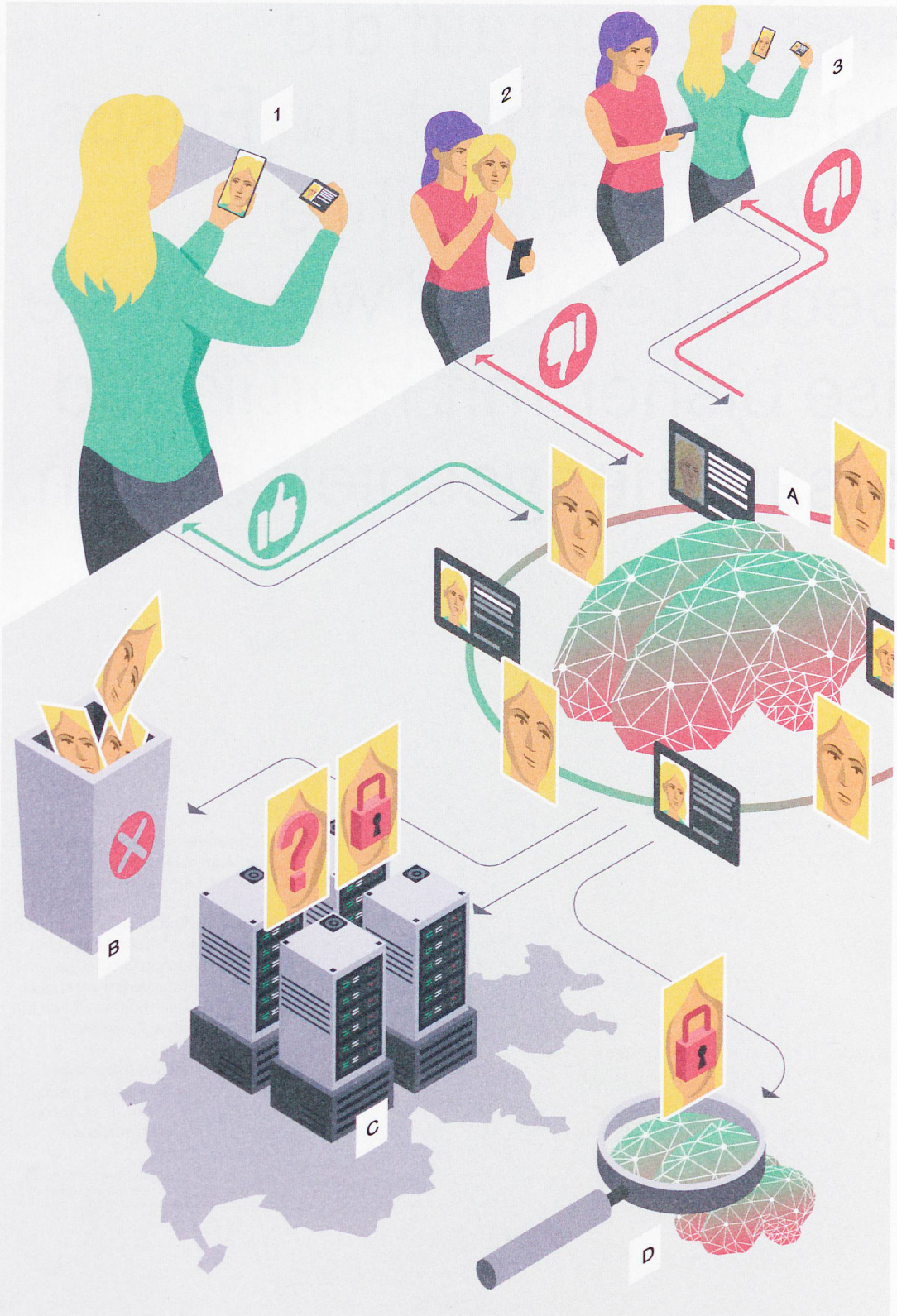
So funktioniert's : trotz Physical Distancing: Anna verifiziert

Trotz Physical Distancing: Anna verifiziert

Die digitale Erkennung der Identität wird immer wichtiger, wobei die Sicherheit der Daten ein Knackpunkt ist. Ein Spin-off der ETHZ hat eine passende Software-Plattform entwickelt.

Text Judith Hochstrasser **Illustration** Ikonaut



Missbrauch erkannt!

(1) Anna will ein neues Mobilabo lösen. Wegen des Lockdowns kann sie nicht persönlich in den Laden. Das Unternehmen PXL Vision bietet dafür eine Software an. Anna kann via mobile App ihre ID einscannen. Danach muss sie ein Selfie-Video machen. Die Eingaben werden von Algorithmen überprüft.

(2) Geht es bei Annas Identifizierung mit rechten Dingen zu? Nein, hier steht eigentlich Lisa. Sie hat die ID von Anna geklaut und sich für das Selfie-Video ein Foto von Anna als Maske übers Gesicht gelegt. Die Algorithmen erkennen die Fälschung.

(3) Lisa könnte Anna auch mit der Pistole zu einem Abo zwingen. Die Forschenden des Spin-offs der ETH Zürich arbeiten deswegen daran, dass die Algorithmen in den Gesichtern Emotionen wie Angst eindeutig erkennen.

Alles sicher?

(A) Annas ID und ihr Selfie-Video werden im Smartphone selbst, auf dem Server des Spin-offs oder jendem des Mobilfunkanbieters abgeglichen. Die Verifizierung basiert auf Deep-Learning-Algorithmen, die Gesichter prüfen, Lebendigkeit erkennen, Texte extrahieren. Das Spin-off muss die Sicherheit der hochsensiblen Bilddaten gewährleisten.

(B) Manchmal werden die Daten nach dem Abgleich sofort wieder gelöscht.

(C) Gewisse Kunden von PXL Vision wie etwa Mobilfunkanbieter und Banken müssen die Daten jedoch per Gesetz speichern. Das Spin-off selbst braucht zudem authentische Bilder und Videos, um seine Algorithmen weiterzuentwickeln. Annas ID und Video landen deswegen verschlüsselt und anonymisiert in einem Schweizer Datencenter, wo sie in separaten Datenbanken gespeichert werden.

(D) Um die Sicherheit weiter zu erhöhen, forscht das Spin-off daran, wie Algorithmen dereinst mit verschlüsselten Bilddaten trainiert werden können.