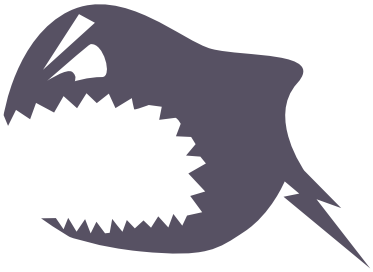
Doxing – too much information



Mitten in der Nacht klingelt es bei einer jungen Frau – vor der Tür stehen Menschen, die bei ihr Party machen wollen. Es werden immer mehr, gleichzeitig wird ihr Smartphone geflutet von Nachrichten fremder Personen. Sie hat keine Ahnung, was da gerade passiert, bekommt Panik, schließt sich ein. Später stellt sich heraus: Jemand hat über einen Messenger-Dienst private Daten der Frau veröffentlicht – und Unbekannte zu einer angeblichen Party bei ihr zu Hause eingeladen.
Ein anderes Beispiel: 2019 werden private Adressen, Telefonnummern und E-Mail-Adressen von vielen Politikerinnen und Politikern sowie Prominenten ins Internet gestellt – und zwar ohne dass diese zugestimmt hatten. Man findet heraus: Ein junger Mann hatte die vielen personenbezogenen Daten zusammengetragen und veröffentlicht.

Solche Angriffe auf die Privatsphäre im digitalen Raum nennt man *Doxing*. Darunter versteht man das gezielte Sammeln und Veröffentlichen von personenbezogenen Daten im Internet, ohne dass die betroffene Person damit einverstanden ist und davon weiß. Oft geht es dabei nicht nur um Informationen wie Name, Geburtsdatum, Adresse, sondern auch um Kontodaten, private Chats und Fotos, die nicht für die Öffentlichkeit bestimmt sind – und um die Namen und Adressen von Familie oder Freundinnen und Freunden. All das kann ausgesprochen unangenehm werden und Konsequenzen haben – von Peinlichkeiten ohne Ende und Ärger mit anderen bis hin zu Mobbing, Stalking und direkten Angriffen. Es kann psychische und physische Folgen für die Doxing-Opfer haben – sie haben Angst, fühlen sich zu Hause und in der Öffentlichkeit nicht mehr sicher.

Woher kommt der Begriff *Doxing*?
Das Wort Doxing leitet sich von der englischen Abkürzung *dox* für *documents* (dt. ‚Dokumente‘) ab. Seinen Ursprung soll Doxing in der Anfangszeit des Internets haben, als rivalisierende anonyme Hackerinnen und Hacker die Identität ihrer Konkurrenz ausgespäht und preisgegeben haben sollen. Heute steht der Begriff generell für die digitale Veröffentlichung persönlicher Informationen.

Woher kommen die Daten?

Die Daten, die beim Doxing missbraucht werden, stammen aus verschiedenen Quellen.

Öffentlich zugängliche Daten
Viele Menschen veröffentlichen selbst (mehr oder weniger) freiwillig viele Informationen im Internet – vor allem, wenn sie auf Social Media aktiv sind. Sie geben Geburtsdatum und Wohnort an, haben eine öffentlich sichtbare Freundesliste, posten Fotos und Filme, die sie dann auch oft noch kommentieren und beschreiben. Da Userinnen und User im Internet häufig entweder direkt ihren echten Namen verwenden oder aber bei verschiedenen Portalen denselben Alias-Namen, können andere schnell alle Profile einer Person zusammentragen.

Hat jemand zusätzlich eine Internetseite, so sind dort oft auch Informationen wie die private Adresse, Schulausbildung oder Arbeitgeber zu finden.

Oft ist es zudem einfach möglich, die Metadaten von Fotos herauszufinden, die jemand im Internet etwa in seinen Social-Media-Kanälen veröffentlicht. Solche Metadaten sind Informationen zu einem Foto, etwa wo und wann es gemacht und veröffentlicht wurde. Wenn jemand oft und regelmäßig Bilder postet, können Dritte daraus relativ einfach ein Bewegungsprofil (also wann die Person wo war) erstellen. Vielleicht erkennen sie auch regelmäßige Aufenthaltsorte. Außerdem sind manche Menschen etwa in Jahrbüchern, in Telefonbüchern oder auf Webseiten der Schule, der Arbeit oder von Vereinen zu finden.

Aus all diesen öffentlichen Daten und Fotos können Dritte also zahlreiche Schlüsse ziehen, z. B. über Hobbys, Vorlieben, Reisen, Aufenthaltsorte – und daraus systematisch ein Profil einer Person erstellen (und veröffentlichen).

Illegal beschaffte Daten

Doch Doxing beschränkt sich nicht immer darauf, öffentlich verfügbare Daten zu sammeln – manche Täterinnen und Täter gehen noch weiter und versuchen auf kriminelle Art und Weise, an Daten zu kommen: etwa über gehackte Konten, Schadprogramme oder so genannte Social Engineering-Methoden. Diese Methoden funktionieren ähnlich wie ein Trickbetrug per Telefon oder an der Haustür: Auf scheinbar seriöse Art und Weise wird nach bestimmten Informationen und Zugangsdaten etwa für E-Mail-, Bankaccounts oder Social-Media-Konten gefragt, um dann Daten auszuforschen, Inhalte zu veröffentlichen oder auch Konten leerzuräumen. Bekannte Tricks sind z. B. die Warnung vor einer Kontosperrung, besonders günstige Kaufangebote oder Gewinnversprechen, wenn man persönliche Daten eingibt. Diese Betrugsmasche wird auch Phishing genannt. Ein solcher Datenklau kann auch dazu führen, dass Fremde auf Kosten des Opfers online einkaufen oder den Namen nutzen, um andere zu täuschen.

Welches Ziel hat Doxing?

Doxing kann viele Motive haben – von Spaß, Bloßstellung und Rache über Einschüchterung und Stalking bis hin zur Erpressung mit der Drohung, weitere Daten zu veröffentlichen.

Bei „harmlosen“ Fällen wird lediglich auf den Namen einer anderen Person eine Pizza bestellt. Oft werden aber auch sehr private Informationen gezielt an bestimmte Kreise weitergegeben, etwa an die ganze Schulklasse. Alle können sich vermutlich gut vorstellen, wie unangenehm es ist, wenn private Chats oder Fotos öffentlich gemacht werden, die nur für einen kleinen privaten Kreis gedacht waren. In anderen Fällen mündet Doxing in Stalking, bei dem ganze Familien belästigt werden. Es kann auch zu öffentlichen Demütigungen, Cybermobbing und Bedrohungen führen.

Manchmal geht es beim Doxing auch um Hass und Diskriminierung. Manche Täterinnen und Täter greifen gezielt Personen aus Minderheitengruppen an. Genauso werden Prominente, Politikerinnen und Politiker sowie Führungskräfte von Unternehmen immer wieder Opfer von Doxing, indem private Details veröffentlicht werden, die ihrem Ruf nachhaltig schaden können oder die sogar zu Bedrohungen führen. Immer wieder werden Listen mit Adressen und anderen Daten veröffentlicht. Bekannt wurde auch die so genannte GamerGate-Kampagne

2014 um Sexismus im Gaming, in der es nach der Veröffentlichung von privaten Daten von Spieleentwicklerinnen sogar Morddrohungen gab.

Ziel von Doxing ist häufig, Menschen Angst einzujagen und sie zum Schweigen zu bringen. Häufig werden Politikerinnen und Politiker oder Aktivistinnen und Aktivisten angegriffen. Manchmal trifft es Menschen aber auch zufällig.

Ist Doxing verboten?

Das Sammeln von öffentlich zugänglichen Daten ist zunächst einmal nicht strafbar. Anders kann das Verbreiten ohne das Einverständnis der Betroffenen bewertet werden – vor allem natürlich, wenn die Daten auf illegale Weise beschafft wurden. So ist das „gefährdende Verbreiten personenbezogener Daten“ seit einigen Jahren verboten. Wer öffentlich Daten verbreitet, die Menschen in die Gefahr bringen, Opfer eines Verbrechens oder einer anderen rechtswidrigen Tat zu werden, der muss mit einer Geld- oder Gefängnisstrafe rechnen – bei illegal beschafften Daten sogar bis zu drei Jahre.[1]

Viele Internetplattformen sind aktiv geworden und verbieten in ihren Richtlinien, Daten anderer ohne deren Zustimmung zu posten. Verstöße können den Plattformbetreibern gemeldet werden. Auf TikTok heißt es beispielsweise: „Inhalte, die als illegal gemeldet werden, werden zunächst anhand unserer Richtlinien überprüft und weltweit entfernt, wenn sich herausstellt, dass der Inhalt gegen die Richtlinien von TikTok verstößt.“[2] Auch bei Instagram kann man jeden Beitrag melden: „Wenn ein*e andere*r Nutzer*in deine privaten Daten auf Instagram gepostet hat, solltest du dich direkt an ihn*sie wenden, um die Löschung dieser Daten anzufordern. Sollte eine andere Person dich bitten, ihre privaten Daten zu löschen, respektiere bitte ihre Privatsphäre und lösche den Inhalt, um zu vermeiden, dass Instagram dein Konto gemeldet wird.“[3]

Doch generell ist die Suche nach möglichen Täterinnen oder Tätern im Internet schwierig – unter anderem, weil Telekommunikationsanbieter aus Datenschutzgründen viele Daten nach wenigen Tagen löschen müssen.

Was kann man gegen Doxing tun?

Generell sollte man im digitalen Raum sehr sparsam mit den eigenen Daten umgehen und so wenig persönliche Informationen veröffentlichen wie möglich. Wichtig ist es, die Sicherheitseinstellungen von Social Media-Accounts, Smartphone und Computer regelmäßig zu überprüfen. Und: Bei Fragen per Mail oder auch am Telefon nach Zugangsdaten oder PINs sollte man immer misstrauisch sein und im Zweifel lieber die Antwort verweigern – und erstmal die angeblichen Absenderinnen oder Absendern fragen, ob die Anfrage wirklich von ihnen kommt.

Mit folgenden Tipps kannst du dich vor Doxing schützen:

- Nutze für Social Media-Konten eine E-Mail-Adresse, in der dein echter Name nicht vorkommt.

[1] vgl. StGB § 126.
[2] TikTok (2024): Illegale Inhalte melden.
[3] Instagram-Nutzungsbedingungen (2024): Private Daten veröffentlichen.

- Benutze für verschiedene Social-Media-Konten unterschiedliche Nutzernamen. So kann man nicht so einfach Informationen über dich sammeln. Achte auch darauf, dass du unterschiedliche und sichere Passwörter für deine Konten erstellst.
- Halte deine Social Media-Konten privat und akzeptiere nur Follower-Anfragen von Menschen, die du kennst.
- Teile auf Social Media möglichst wenige persönliche Informationen wie deinen vollständigen Namen, das Geburtsdatum, den Wohnort, deine Schule etc.
- Überprüfe regelmäßig deine Privatsphäre-Einstellungen. Am besten sollten deine Profile so privat wie möglich sein.
- Teste selbst, wie viele Informationen du im Internet über dich finden kannst, zum Beispiel mit einer Google-Recherche oder indem du dich von deinen Konten abmeldest und sie dir aus der Perspektive einer oder eines „Fremden“ anschaust.

Wenn du gedoxt wurdest, solltest du dir professionelle Hilfe suchen. Du kannst dich an Vertrauenspersonen wie Eltern oder Lehrkräfte wenden, aber auch an Beratungsstellen (z. B. Juuuport) oder die Polizei, bei der du Anzeige erstatten kannst. Um Beweise zu sichern, ist es wichtig, rechtssichere Screenshots von Privatnachrichten oder Postings zu machen. Natürlich sollte man auch die Möglichkeiten der Plattformen nutzen, die Doxing-Beiträge melden.