POSITIONSPAPIER

Künstliche Intelligenz für den öffentlichen Sektor: Masked Federated Learning als datenschutzfreundliche Lösung

Martin Schallbruch
(Digital Society Institute der ESMT Berlin)

Professor Michael Huth
(Imperial College London, Xayn AG)

Dr. Leif-Nissen Lundbæk
(Xayn AG)

Dr. Clara Herdeanu
(Xayn AG)

Lola Attenberger
(Digital Society Institute der ESMT Berlin)

DSI | DIGITAL SOCIETY INSTITUTE BERLIN

ESMT BERLIN

Xayn

INHALTSVERZEICHNIS

1. EINSTIEG

Wollen wir Staat und Verwaltung weiterentwickeln, leistungsfähiger und fit für die Zukunft machen, benötigen wir Technologie. Die Corona-Pandemie hat gezeigt, dass die Digitalisierung der Behördenstrukturen in Deutschland, ihre Zusammenarbeit und das digitale Handeln des Staates noch weit hinter den Erwartungen zurückbleiben. In den nächsten Jahren wird es deshalb darauf ankommen, die Behörden in Bund, Ländern und Kommunen konsequent zu digitalisieren.

Künstliche Intelligenz (KI) bietet hierfür große Potenziale. Maschinelles Lernen und KI können maßgeblich dazu beitragen, Entscheidungsprozesse in Behörden, Organisationen und Institutionen optimaler, kostengünstiger, schneller und automatisiert zu gestalten. Die öffentliche Verwaltung kann ihre internen und externen Leistungen mit Hilfe von KI zielgerichteter, passgenauer und einfacher bereitstellen[1]. Jede Form der Digitalisierung öffentlicher Leistungen und der digitalen Zusammenarbeit von Behörden, Unternehmen und Bürger*innen muss **hohe Anforderungen an Datenschutz und Vertrauenswürdigkeit erfüllen**. Unnötige zentrale Datensammlungen, übermäßige Speicherung und Verwendung persönlicher Daten oder intransparente Datennutzung sind mit den Erwartungen der Menschen an Datenschutz und Selbstbestimmung nicht zu vereinbaren und widersprechen auch europäischem Datenschutzrecht. Damit KI im öffentlichen Bereich sinnvoll eingesetzt werden kann und hohen Nutzen für das Gemeinwesen schafft, müssen die innovativen Potentiale der KI mit Datensparsamkeit, Transparenz und Vertrauenswürdigkeit vereint werden.

Neue technische Ansätze stehen hierzu zur Verfügung. Im Folgenden skizzieren die Autor*innen einen der vielversprechendsten Ansätze, das sogenannte **Masked Federated Learning**, und erläutern die Anwendung im öffentlichen Bereich an den Beispielen des Gesundheitswesens und der Strafverfolgung.

[1] *Vgl. Die Bundesregierung (2018): Strategie Künstliche Intelligenz der Bundesregierung. Stand: November 2018. S. 31. Link*

2. MASKED FEDERATED LEARNING:
Dezentrale Technologie mit eingebautem Schutz der Privatsphäre

Um KI-Modelle zu trainieren, werden große Mengen an Daten benötigt – in vielen Fällen auch persönliche Daten. Je mehr solcher persönlichen Daten verwendet werden, desto größer sind die Risiken für die Privatsphäre. Dieses Spannungsverhältnis führt zum „**KI-Privatsphärendilemma**“, was sich bislang wie folgt durchdeklinieren ließ: Je mehr persönliche Daten eingesetzt werden, desto leistungsfähiger und präziser sind die KI-Anwendungen. Wird die Menge der Daten reduziert, um Datenschutzrisiken zu verringern, entsteht minderwertige Technologie, die das Potenzial von KI-basierten Anwendungen nicht ausschöpft.

Eine Lösung für das Dilemma ist **Masked Federated Learning**[2], **eine dezentrale Technologie, die Datenschutz mit leistungsfähiger KI vereint**. Bei diesem Ansatz bleiben die Rohdaten dort, wo sie entstehen – auf den Endgeräten der Nutzer*innen. Statt die Daten zu den Algorithmen zu bringen, werden die Algorithmen zu den Daten geschickt und vor Ort trainiert. Diese auf den lokalen Datensätzen trainierten KI-Modelle werden zu einem globalen Modell aggregiert. Dieses globale Modell ist die Grundlage für nachfolgendes lokales Lernen, indem es die kollektiven Erfahrungen an die lokalen Modelle zurückspielt, sodass eine Form des kollaborativen Lernens stattfindet (vgl. Abb. 1[3]). Im Netzwerk werden lediglich verschlüsselte KI-Modelle kommuniziert und keine sensiblen persönlichen Daten. Da die personenbezogenen Rohdaten die Endgeräte zu keinem Zeitpunkt verlassen, wird die kostspielige und technisch wenig überzeugende Anonymisierung der Daten überflüssig.

Föderiertes maschinelles Lernen **erfüllt deshalb die Anforderungen von Datenschutzrichtlinien wie der DSGVO**. Zusätzlich bietet der Ansatz den Vorteil, dass das Lernen asynchron stattfinden kann, da die

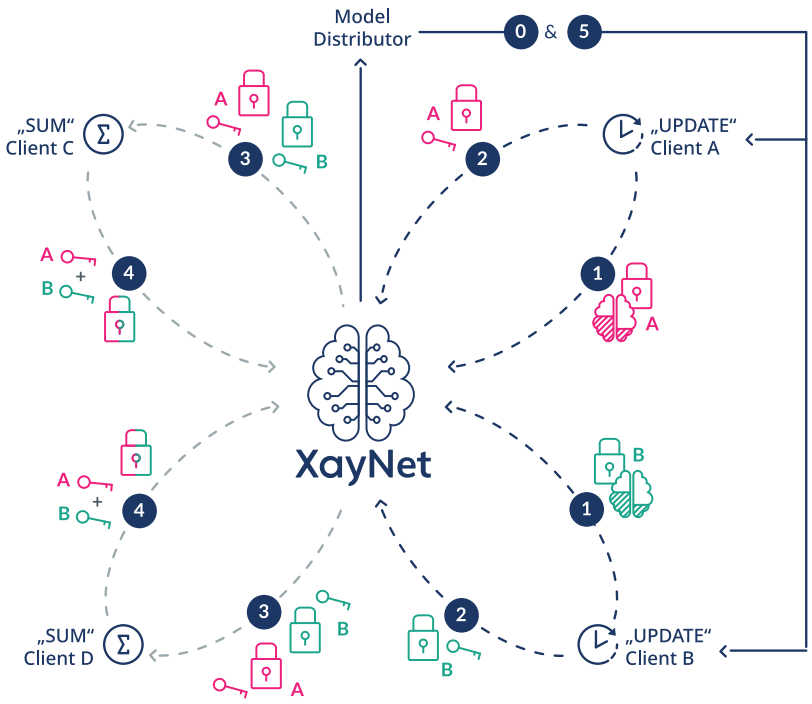

Abb. 1: Masked Federated Learning (Quelle: Xayn AG)

[2]*Vgl. Dänschel, L.; Huth, M.; Lundbæk, L. (2020): XayNet: Masked Cross-Device Federated Learning Framework. Link*
[3]*Ebd. S. 16.*

einzelnen lokalen Modelle relativ unabhängig voneinander agieren. Denn aufgrund des exponentiellen Wachstums globaler Datenströme ist es nicht nachhaltig, all diese Informationen für weitere Verarbeitung zentral zu speichern. Asynchrones dezentrales Lernen skaliert weit besser mit den wachsenden Datenmengen. Vorteile bietet der Ansatz auch für die IT-Sicherheit: Potenzielle Angreifer müssten eine Vielzahl an unterschiedlichen Endgeräten gleichzeitig ins Visier nehmen, um erfolgreich zu sein.

Föderiertes maschinelles Lernen kann somit die wachsenden Datenströme in geeignete KI-Modelle verdichten, den **Schutz der Daten gewährleisten**, die **Leistungsfähigkeit und Resilienz der KI sicherstellen und gleichzeitig hoch skalierbar** sein.

Möglich sind sowohl „cross-silo“-Anwendungsfälle, also silo-übergreifende Lösungen, bei denen eine kleinere Zahl an Datensätzen in leistungsfähigen Umgebungen wie Servern gehostet werden, als auch „cross-device“-Anwendungsfälle, bei denen geräteübergreifende Lösungen mit vielen Millionen Einzelgeräten umgesetzt werden. Die gespeicherten Datensätze können in Größe und Mustern erheblich variieren. Gerade bei den cross-device Ansätzen ist es allerdings wichtig, nicht erst nachträglich von einem zentralen Modell auf ein dezentrales KI-Modell umzusteigen. Sind bereits alle Trainingsdaten in einem zentralen Modell gesammelt, ist die Umstellung auf ein dezentrales Modell sehr viel komplizierter. Cross-device Ansätze erfordern außerdem auch eine minimale Leistungsfähigkeit der Endgeräte, um dort maschinelles Lernen zu ermöglichen.

Die folgenden möglichen Anwendungsbeispiele aus dem Gesundheitssektor und der Strafverfolgung verdeutlichen das **zukunftsweisende Potenzial dieser Methode – gerade für den öffentlichen Sektor mit seinen besonders hohen Anforderungen an Datenschutz und Resilienz**.

3. ANWENDUNGSBEISPIELE aus dem öffentlichen Sektor

3.1. Gesundheitswesen: Nach der Pandemie ist vor der Pandemie

Die Corona-Pandemie hat die Welt auf den Kopf gestellt und global bereits mehr als 3 Millionen Todesopfer[4] gefordert. Internationale Expert*innen warnen bereits, dass wir in eine Ära der Pandemien eingetreten sind und diese zukünftig häufiger auftreten und dabei schneller sowie tödlicher verlaufen[5]. Die Covid-19-Pandemie muss als Warnschuss für zukünftige Pandemien verstanden werden. Entscheidungsträger*innen sollten sich auf weitere Ernstfälle vorbereiten. In Deutschland hat der Kampf gegen Covid-19 der Digitalisierung einen enormen Schub gegeben, gleichzeitig aber auch digitale Schwächen unseres Landes offenbart – zum Beispiel beim Einsatz neuer Technologien für das öffentliche Gesundheitswesen.

Die Corona-Warn-App hat gezeigt, dass dezentrale Technologien datenschutzfreundlich dabei helfen können, die eigene und die öffentliche Gesundheit zu schützen. Solche Ansätze sollten weiter ausgebaut werden. Denkbar ist ein Einsatz der KI, um über Covid-19 hinaus jeder Person ein Instrument in die Hand zu geben, das individuelle Risiko von Infektionserkrankungen zu erkennen. Eine digitale Anwendung, die auf dem dargestellten föderierten Lernen basiert, kann auf Grundlage der jeweiligen Ausgangsbedingungen wie körperliche Konstitutionen, Geschlecht, Alter, regionales Infektionsgeschehen, bestehende Kontakte mit (potenziell) infizierten Personen und Impfstatus eine KI-basierte Einschätzung liefern. Die hoch sensiblen persönlichen Daten bleiben dabei auf den Endgeräten der Nutzer*innen, während lediglich die verschlüsselten KI-Modelle zu einer Nutzungs- und Geräteübergreifenden stetigen Verbesserung der Leistungsfähigkeit verwendet werden.

Zudem werden auf diese Art Einschätzungen gebündelt, um auf systemischer Ebene Rückschlüsse zu potenziellen Infektionsherden und -risiken zu erhalten. Die Gesundheitsämter könnten auf solche kollektiven Ergebnisse zurückgreifen, um besser abschätzen zu können, welche Maßnahmen den besten Gesundheitsschutz ermöglichen. Dazu erhalten und benötigen die Ämter nicht die personenbezogenen Rohdaten.

Sollten im Verlauf einer zukünftigen Pandemie neue wissenschaftliche Erkenntnisse zu Risikofaktoren gewonnen werden, könnten sie in das Modell eingespielt und die aufgrund von exogenen sowie endogenen Faktoren betroffenen Personen individuell gewarnt werden. **Solch ein dezentraler Ansatz in Kombination von cross-device- und cross-silo-Anwendung würde den Einzelpersonen einen besseren individuellen Schutz bieten. Gleichzeitig würden Gesundheitsämter und weitere Behörden befähigt werden, evidenzbasierte Entscheidungen zum Schutz der Bevölkerung zu treffen.**

Je mehr Einzelpersonen solch eine Anwendung installiert haben und aktiv nutzen, desto bessere Entscheidungshilfen könnten die zuständigen Akteure wie Gesundheitsämter oder politische Entscheidungsträger*innen daraus ziehen.

[4]World Health Organization (2021): WHO Coronavirus (Covid-19) Dashboard. Link

[5]Vgl. The Intergovernmental Science Policy Platform on Biodiversity and Ecosystem Services (2020): IPBES Workshop Report on Biodiversity and Pandemics. United Nations Environment Programme. Link

3.2. Strafverfolgung: Früherkennung von Straftaten durch intelligente Datenanalyse

In einer weitgehend digitalisierten Welt ist die Analyse von massenhaft vorliegenden digitalen Daten ein notwendiges und wirksames Mittel der polizeilichen Arbeit. Auffälligkeiten in Datenbeständen können dabei helfen, Straftaten frühzeitig zu erkennen, vorliegende Verdachtsfälle zu bestätigen oder der Strafverfolgung neue Ermittlungsansätze zu ermöglichen. Die Polizei kann hierzu auf unterschiedliche Datenquellen zurückgreifen.

Im Rahmen des Projekts Polizei 2020 soll ein Datenhaus der deutschen Polizei entstehen (vgl. Abbildung 2)[6], in dem ein gemeinsamer bundesweiter Datenbestand (vgl. Abbildung 2, grün) ergänzt wird durch Datenbestände der einzelnen Polizeibehörden. Der gemeinsame Bestand wird zukünftig größer sein (können) als heute, gleichwohl steht aber nicht das ganze Wissen der Polizeibehörden allen anderen Behörden zur Verfügung.

Bearbeiten Polizeibeamt*innen einen Fall, erheben sie vor Ort zahlreiche digitale Daten, die für den jeweiligen Fall relevant sind – darunter zum Beispiel Daten aus Recherchen in sozialen Netzwerken, von beschlagnahmten Geräten und Datenträgern, aus Funkzellenabfragen oder aus der Telekommunikationsüberwachung. Daneben können die Strafverfolgungsbehörden fallbezogen oder generell auf vorhandene staatliche Datenbestände zugreifen, beispielsweise die Melde- oder Fahrzeugregister. Schließlich gibt es eine Reihe von gesetzlich normierten Verdachtsanzeigen, die Unternehmen verpflichtet, direkt oder indirekt digitale Daten an die Strafverfolgungsbehörden zu liefern, um bestimmte Straftaten frühzeitig erkennen zu können. Dazu gehören Verdachtsanzeigen von Banken zur Geldwäscheprävention oder Verdachtsanzeigen von Betreibern sozialer Netzwerke zu Hasskriminalität. Darüber hinaus sollen Internetanbieter zukünftig auch verpflichtet werden, bestimmte Cyberstraftaten an das BKA zu melden.

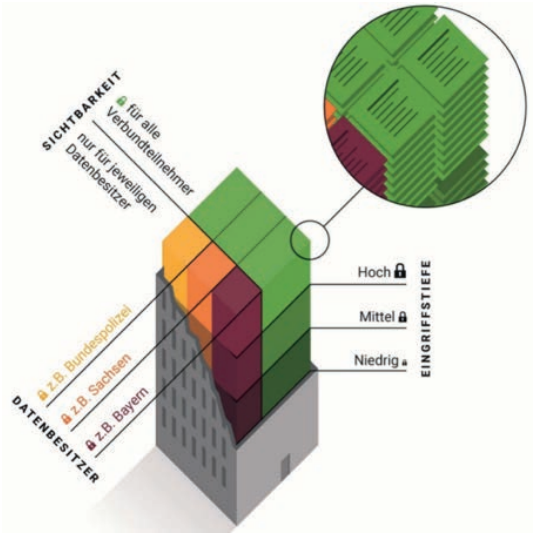

Abb. 2: Datenhaus der deutschen Polizei (Quelle: Bundesministerium des Inneren[7])

Polizeibehörden stehen vor der Aufgabe, die eingehenden Informationen zu analysieren und zu bewerten, woraus sich Anhaltspunkte für potenzielle Straftaten ergeben. **Angesichts der wachsenden Fülle und Vielfalt der Informationen ist hierzu ein hoher Automatisierungsgrad erforderlich**. Informationen müssen im ersten Schritt möglichst automatisch daraufhin klassifiziert werden, ob sie für einen bestimmten Phänomenbereich überhaupt relevant erscheinen. Nur wenn dies der Fall ist, sollten die Informationen gegebenenfalls noch manuell überprüft und Ermittlungen durchgeführt werden. Eine solche initiale Klassifizierung von Informationen unterscheidet sich je nach Phänomenbereich und Art der Information.

Bei Delikten, die mit Bildern sexualisierter Gewalt gegen Kinder und Jugendliche[8] zu

[6] *Bundesministerium des Innern: Polizei 2020. White Paper, Januar 2018. Link*

[7] *Bundesministerium des Innern: Polizei 2020. White Paper, Januar 2018, S. 12. Link*

[8] *Die Autor*innen verwenden hier ganz bewusst nicht die geläufige Formulierung „Kinderpornographie", da diese Formulierung die dahinterstehende sexualisierte Gewalt gegen Kinder und Jugendliche verharmlost – vgl. auch Frauen gegen Gewalt e.V.: Hinweise für die Berichterstattung über Gewalt gegen Frauen und Kinder. Link*

tun haben, muss zunächst geprüft werden, welche Bilder überhaupt Anhaltspunkte für ein Verbrechen liefern können. Um Geldwäsche zu erkennen, müssen zunächst aus einer Menge von Zahlungsverkehrsdaten diejenigen Datensätze ermittelt werden, die für eine weitere Analyse relevant sind. Um wegen betrügerischer eCommerce-Aktivitäten zu ermitteln, müssen aus einer Menge gesicherter Kommunikationsdaten diejenigen herausgefiltert werden, die bestimmten Mustern betrügerischer Transaktionen entsprechen.

Die Qualität solcher initialen, weitgehend automatisch durchzuführenden Analysen digitaler Daten hängt stark davon ab, ob und in welchem Maße es gelingt, polizeiliches Erfahrungswissen über die jeweiligen Delikte und ihre spezifischen Begehungsformen und Begleitumstände einzubeziehen. Alle beispielhaft genannten Delikte zeichnen sich durch bestimmte Modi Operandi aus, die zur Klassifikation der Informationen genutzt werden können. Welche Art von Darstellungen sind bei Abbildungen sexualisierter Gewalt gegen Kinder und Jugendliche üblich? Welche Transaktionen haben ein hohes Potenzial für Geldwäsche? Welche Anfragemuster zeichnet Bots aus, die Online-Händler betrügen wollen? Solche polizeilichen Erfahrungswerte verfestigen sich mit der Anzahl der Fälle, die bearbeitet werden. Gleichzeitig müssen sie offen sein für eine dynamische Weiterentwicklung, da neue Begehungsformen schnell adaptiert werden müssen.

KI kann dabei unterstützen, diese Daten zu analysieren und zu klassifizieren – wie bereits verschiedene Projekte bei deutschen Sicherheitsbehörden aufzeigen[9]. Die bisher begonnenen Projekte bewegen sich innerhalb der Zuständigkeit einer einzelnen Sicherheitsbehörde und beziehen sich auf ein bestimmtes Kriminalitätsphänomen. Dieses eher punktuelle Vorgehen nutzt die Potenziale nicht, die in dem gesammelten Erfahrungswissen aller Polizeibehörden liegen.

Sinnvoll wäre daher eine Lösung, die KI-Unterstützung bei der Klassifikation von Informationen in einer Art und Weise anbietet, bei der das Erfahrungswissen aller Behörden gesammelt eingebracht werden kann. Doch nur bei besonders schweren Straftaten und mit ausdrücklicher gesetzlicher Ermächtigung ist es möglich, alle phänomenbezogenen Daten aller Polizeibehörden zusammenzuführen, um umfassende KI-Modelle zu entwickeln.

Der Ansatz des föderierten Lernens bietet eine Lösung, **nicht die persönlichen Informationen zwischen den Behörden auszutauschen, sondern allein das Erfahrungswissen in der Klassifikation von Informationen**. So profitiert eine Polizeibehörde von dem Erfahrungswissen anderer Behörden. Damit vergrößert sich das Erfahrungswissen der Polizeien insgesamt, ohne dass alle persönlichen Daten zusammengeführt werden. Die dezentralen Modelle trainieren gemeinsam ein zentral vorgehaltenes Modell, das allen Polizeibehörden zur Verfügung steht. Das zentrale Modell wird dann wiederum genutzt, um die lokalen Modelle zu verbessern – und **alles, ohne dass die Polizeien die personenbezogenen Rohdaten miteinander teilen müssen**.

[9]Aktuelle KI-Projekte deutscher Sicherheitsbehörden sind zum Beispiel die automatisierte Bilderkennung bei Ermittlungen zu sexualisierter Gewalt gegen Kinder und Jugendlichen (StA Köln, vgl. Behördenspiegel, Januar 2021, S. 29) oder das KI-basierte System „FIU Analytics" der Financial Intelligence Unit (FIU) zur Geldwäscheerkennung (vgl. Handelsblatt, 24. November 2020).

4. AUSBLICK

Manche sehen die Europäische Union wegen ihrer Datenschutzregulierung als wahrscheinlich vertrauenswürdigste Region der Welt und betrachten dies als Wettbewerbsvorteil[10]. Andere sehen den Datenschutz als innovationshemmend[11] oder sogar schädigend in Pandemiezeiten[12]. Das hier erläuterte **Masked Federated Learning eignet sich optimal, um den Schutz personenbezogener Daten mit dem Nutzen dieser Daten in Einklang zu bringen**. Als dezentralisierte selbstlernende Technik verfolgt das föderierte Lernen einen **Privacy-by-Design-Ansatz**, da keine persönlichen Daten zentral zusammengeführt werden müssen. Die Speicherung der Daten erfolgt nur lokal.

Damit kann die Umsetzung der KI-Strategie der Bundesregierung[13] unterstützt werden, die einerseits weitere Anwendungen, vor allem auch im öffentlichen Sektor fördert, andererseits besonderen Wert auf die grundrechtskonforme Ausgestaltung der KI-Anwendung in jedem einzelnen Anwendungsfall legt. Die Regierung strebt an, Daten innovativ zu nutzen, ohne dabei den Datenschutz zu gefährden[14].

Für die Gesundheitsversorgung und Pflege geht es der Regierung nicht nur um Forschungsprojekte, sondern um eine datenunterstützte Gesundheitsversorgung, die KI-Werkzeuge im Alltag unterstützen. Das Beispiel für den Einsatz von föderiertem Lernen im Gesundheitssektor zeigt, **wie mit dieser Technik in künftigen Pandemien Risiken schnell erkannt und eingedämmt sowie eine schnellere Reaktionsfähigkeit gewährleistet werden** könnte. Die kollaborative, dezentralisierte Technik könnte Bürger*innen und Gesundheitsämter im Informationsaustausch und bei der Datenanalyse unterstützen. Das System könnte Bürger*innen ermöglichen, schneller und informierter Risiken einzuschätzen. Gleichzeitig könnte die Kommunikation zwischen den Behörden untereinander sowie mit den Service-Nutzer*innen deutlich verbessert werden. Für die öffentliche Sicherheit betrachtet die Bundesregierung KI als strategisches Instrument, die Leistungsfähigkeit der deutschen Polizei weiter zu erhöhen, zum Beispiel bei hybriden Bedrohungen. Die gezeigten Beispiele verdeutlichen, dass das **föderierte Lernen die Arbeit der Polizei insgesamt erleichtern könnte, ohne Daten zentral zusammenzuführen**. Gerade eine grundsätzlich problematische Weitergabe persönlicher Daten im Vorfeld konkreter Verdachtsmomente könnte vermieden werden, gleichwohl aber maschinelles Lernen genutzt werden, um polizeiliche Verdachtsgenerierung zu unterstützen.

Insgesamt zeigten die hier darstellten Einsatzfälle in der Gesundheitsverwaltung und bei der Polizeiarbeit, welches Potenzial ein dezentral organisiertes selbstlernendes System für die öffentliche Verwaltung bietet. Die Verwaltungsservices für die Bürger*innen könnten durch das föderierte Lernen verbessert werden, denn die **Technologie hat das Potenzial die Effizienz zu steigern und das Vertrauen der Bürger*innen in die Verwaltung zu stärken**. Masked Federated Learning könnte so ein **EU-Modell zur verantwortungsvollen KI-Nutzung** werden. Alle Vorteile maschinellen Lernens können ausgenutzt werden – und gleichzeitig bleibt der **Schutz der persönlichen Daten** gewahrt.

[10] *Vgl. Dreo, G.; Eiseler, V.; Gentschen Felde, N.; Gehrke, W.; Helmbrecht, U.; Hommel, W.; Zahn, J. (2020): Europäische Digitale Souveränität: Weg zum Erfolg? – Ein Bericht zur Jahrestagung CODE 2020. In: Z Außen Sicherheitspolitik 13: 399-404. Link*

[11] *Vgl. Mertens, P. (2019): Die Datenschutz-Grundverordnung – eine kritische Sicht. In: Wirtschaftsinformatik & Management, 11(1): 6-17. Link*

[12] *Vgl. Hottelet, U. (2021): Corona-Pandemie: Bremst uns der Datenschutz aus? Link*

[13] *Vgl. Die Bundesregierung (2020): Strategie Künstliche Intelligenz der Bundesregierung. Fortschreibung 2020. Stand: Dezember 2020. S. 22. Link*

[14] *Ebd.*

5. QUELLENVERZEICHNIS

- Dänschel, L.; Huth, M.; Lundbæk, L. (2020): XayNet: Masked Cross-Device Federated Learning Framework. Online: https://uploads-ssl.webflow.com/5ea197660b956f76d26f0026/5fcf7f97c0333cb84277fcd8_XayNet%20Whitepaper%203.0%20v3.pdf
- Bundesministerium des Inneren (2018): Polizei 2020. White Paper, Januar 2018. Online: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/polizei-2020-white-paper.html
- Die Bundesregierung (2018): Strategie Künstliche Intelligenz der Bundesregierung. Stand: November 2018. Online: https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-der-bundesregierung.pdf?__blob=publicationFile&v=10
- Die Bundesregierung (2020): Strategie Künstliche Intelligenz der Bundesregierung. Fortschreibung 2020. Stand: Dezember 2020. Online: https://www.bmwi.de/Redaktion/DE/Publikationen/Technologie/strategie-kuenstliche-intelligenz-fortschreibung-2020.pdf?__blob=publicationFile&v=10
- Dreo, G.; Eiseler, V.; Gentschen Felde, N.; Gehrke, W.; Helmbrecht, U.; Hommel, W.; Zahn, J. (2020): Europäische Digitale Souveränität: Weg zum Erfolg? – Ein Bericht zur Jahrestagung CODE 2020. In: Z Außen Sicherheitspolitik 13: 399-404. Online: https://link.springer.com/article/10.1007%2Fs12399-020-00829-2
- Feldmann, M; Proll, Uwe (2021): Kein Ersatz für den Menschen. In: Behördenspiegel, Januar 2021, S. 29. Online: https://issuu.com/behoerden_spiegel/docs/2021_januar
- Frauen gegen Gewalt e.V.: Hinweise für die Berichterstattung über Gewalt gegen Frauen und Kinder. Online: https://www.frauen-gegen-gewalt.de/de/ueber-uns/presse/informationen-fuer-die-presse/hinweise-fuer-die-berichterstattung-ueber-gewalt-gegen-frauen-und-kinder.html
- Hottelet, U. (2021): Corona-Pandemie: Bremst uns der Datenschutz aus? Online: https://www.heise.de/news/Corona-Pandemie-Bremst-uns-der-Datenschutz-aus-5042875.html
- Mertens, P. (2019): Die Datenschutz-Grundverordnung – eine kritische Sicht. In: Wirtschaftsinformatik & Management, 11(1): 6-17. Online: https://link.springer.com/article/10.1365/s35764-019-0159-5
- Stiens, T. (2020): Wie Software künftig bei der Geldwäsche-Bekämpfung helfen soll. In: Handelsblatt 24.November 2020. Online: https://www.handelsblatt.com/politik/deutschland/finanzkriminalitaet-wie-software-kuenftig-bei-der-geldwaesche-bekaempfung-helfen-soll/26596064.html?ticket=ST-5862866-XOIrpKJFJNMLfhA1nftg-ap3
- The Intergovernmental Science Policy Platform on Biodiversity and Ecosystem Services (2020): IPBES Workshop Report on Biodiversity and Pandemics. United Nations Environment Programme. Online: https://www.unep.org/resources/report/ipbes-workshop-report-biodiversity-and-pandemics
- World Health Organization (2021): WHO Coronavirus (Covid-19) Dashboard. Online: https://covid19.who.int/

ÜBER XAYN
www.xayn.com

Xayn ist eine sichere Suchmaschine, die Nutzer*innen Kontrolle über die Algorithmen gibt und transparent personalisierte Suchergebnisse liefert. Xayn basiert auf aktueller Forschung zu datenschutzfreundlicher Künstlicher Intelligenz aus Europa und hat das Ziel, über nutzerfreundliche Privatsphäre-Technologie Datenschutz für alle zugänglich zu machen.

Das KI-Unternehmen begann als Forschungsprojekt von Dr. Leif-Nissen Lundbæk und Professor Michael Huth an der Universität Oxford und dem Imperial College London. Zusammen mit Felix Hahmann gründeten sie 2017 das Technologieunternehmen. Der akademische Hintergrund spiegelt sich auch im 27-köpfigen Team, das aus 30 Prozent promovierten Wissenschaftler*innen besteht. Das Berliner Unternehmen entwickelte die Open-Source-Plattform XayNet für Federated Learning und Analytics, auf der auch die Suchmaschine Xayn basiert. Earlybird VC und Dominik Schiener investierten in das Unternehmen, das bereits mit Porsche, Daimler, der Deutschen Bahn und Siemens arbeitete.

ÜBER DIE ESMT BERLIN
esmt.berlin

Die ESMT Berlin ist die höchstplatzierte Business School in Deutschland und die erste und einzige deutsche Wirtschaftsuniversität in den europäischen Top 10. Von 25 führenden globalen Unternehmen gegründet, bietet die ESMT Master-, MBA- und PhD-Studiengänge sowie Managementweiterbildung an. Die Kurse werden auf dem Berliner Campus, an Standorten weltweit, online sowie als Onlinekurse mit Teilpräsenz angeboten. Mit einem Fokus auf Leadership, Innovation und Analytics veröffentlichen die Professorinnen und Professoren der ESMT regelmäßig ihre Forschungsergebnisse in führenden wissenschaftlichen Zeitschriften. Zusätzlich bietet die ESMT eine Plattform für den Diskurs zwischen Politik, Wirtschaft und Wissenschaft. Die ESMT ist eine staatlich anerkannte private wissenschaftliche Hochschule mit Promotionsrecht, akkreditiert von AACSB, AMBA, EQUIS und FIBAA, und engagiert sich für Vielfalt, Gleichstellung und Inklusion in all ihren Aktivitäten und Gemeinschaften.

ÜBER DAS DIGITAL SOCIETY INSTITUTE

Das Digital Society Institute (DSI) ist ein interdisziplinäres Forschungsinstitut der ESMT Berlin, das unterstützt von führenden globalen Unternehmen 2015 gegründet wurde. Es begleitet die wirtschaftliche und gesellschaftliche Gestaltung der Digitalisierung durch strategische Forschung und Entwicklung mit einem Schwerpunkt bei der Cybersicherheit.

IMPRESSUM

Herausgeber:
Xayn AG
Unter den Linden 42
10117 Berlin
presse@xayn.com

Redaktion: Dr. Clara Herdeanu

Layout: Julia Hintz

Alle im Text genannten Internetlinks wurden überprüft am 04. Juni 2021.

Berlin, Juni 2021