Augmented Privacy: Fortschritt mit Verantwortung



FACHARTIKEL

_DANIEL NEUBIG
AR Technical Lead
Ergon Informatik AG
_URS ZURBUCHEN
Senior Security Consultant Airlock
Ergon Informatik AG

Erschienen im SMART insights 2021 Magazin

ergon

smart people – smart software®

Die Pandemie hat unsere Kommunikation und das gemeinsame Arbeiten dauerhaft verändert. Dadurch gefördert, hat Augmented Reality (AR) von einem grossen Schub profitiert und die Marktreife erlaubt vielfältige Einsatzzwecke. Die dafür notwendigen Technologien kommen jedoch in Konflikt mit wichtigen Aspekten, insbesondere dem Datenschutz. Es ist in der Verantwortung des AR-einsetzenden Unternehmens, diese Risiken frühzeitig zu behandeln.

Im vergangenen Jahr haben sich die Zusammenarbeit und die sozialen Kontakte zunehmend in den virtuellen Raum verschoben. Durch das verteilte Arbeiten erleben digitale Kommunikationslösungen, Videokonferenzen und auch Projekte mit Augmented Reality einen Schub.

Die Angebote der Marktführer wie Microsoft, Apple, Google, Facebook und Amazon rücken die kommerzielle Nutzung in den Vordergrund und lassen auf das riesige Marktpotenzial schliessen. Neue AR-Anwendungen entstehen rasend schnell und verbessern oder vereinfachen bestehende Lösungen. Spannende Projekte werden umgesetzt und finden hohe Akzeptanz. Analyst:innen gehen sogar von einer jährlichen Wachstumsrate von 100% für Dienste aus, die sich AR zunutze machen.

Unbestritten bietet Augmented Reality viele Vorteile für Unternehmen und Privatanwender:innen. Leider bringen die neuen Technologien aber auch Risiken und potenzielle Verbindlichkeiten mit sich. Sie verwenden sensitive Personendaten, die einer Vielzahl von Gesetzen unterliegen können und Fragen zu Datenschutz und Datensicherheit aufwerfen. Es liegt in der Verantwortung der Unternehmen, dies frühzeitig in ihre digitale Strategie einzubinden.

Das Spiel mit den Daten

Durch den Einsatz von AR wird Nutzer:innen der Zugang zu digitalen Inhalten von Produkten und Dienstleistungen in vielen Branchen stark vereinfacht: Beispielsweise durch Detailinformationen zu Objekten in der Umgebung wie bei virtuellen Fremdenführer:innen in der Touristik, durch schnellere Positionierung von Konstruktionsteilen in der Industrie oder auch mittels Projektion von Computertomografiemodellen während Operationen.

Informationen von vielfältigen Sensoren fliessen in die Anreicherung der Realität mit ein. Neben Positionsdaten und Videoaufnahmen kommen auch biometrische Daten und andere persönliche Informationen zum Tragen. Deren Umfang und Verfügbarkeit bestimmen die Genauigkeit der virtuellen Welt und damit den Nutzen der Lösung.

In unserer Gesellschaft steigt das Datenbewusstsein zunehmend. Zudem reift die Erkenntnis, dass vermeintlich persönliche Situationen oder Konversationen in Wirklichkeit gar nicht so privat sind wie erwartet. Dies fördert Skepsis. Eine erste Begeisterungsphase kann abrupt beendet und die weitere Adaption der neuen Möglichkeiten gehemmt werden. Es entsteht Unsicherheit über die Verwendung anfallender Daten und die Zuverlässigkeit des Schutzes. Insbesondere wird unkontrollierte, missbräuchliche Nutzung in einem anderen, unbewilligten Kontext befürchtet. Oftmals werden auch Informationen über unbeteiligte Dritte erfasst, zum Beispiel, wenn in Bildaufnahmen fremde Gesichter erkennbar werden. Nutzer:innen möchten sich nicht plötzlich mit Verantwortlichkeitsklagen oder Schadensersatzforderungen konfrontiert sehen.

Dieser Privacy-Aspekt des Datenschutzes ist nicht neu. Im Gegenteil, sensitive Daten werden täglich bewusst und unbewusst bei Social Media, Wearables, Smartphones, Internet-of-Things-Lösungen oder

«Dank Transparenz und bewusster Entscheidung können Nutzer:innen zugunsten eines für sie vorteilhafteren Risikoprofils auf Funktionen oder Genauigkeit verzichten.»



_DANIEL NEUBIG, AR TECHNICAL LEAD;
DANIEL.NEUBIG@ERGON.CH

«Marktbeobachtung und stetige Anpassung des Umgangs mit Personendaten sichern die Profitabilität der Lösungen langfristig.»



_URS ZURBUCHEN, SENIOR SECURITY CONSULTANT AIRLOCK;
URS.ZURBUCHEN@ERGON.CH

Smart Homes verarbeitet und gespeichert. Aus solchen Sensordaten, Bildern und Videos lesen Machine-Learning-Algorithmen erkennbare Muster und treffen Annahmen und Entscheidungen. Viele haben sich mittlerweile an diesen Umstand gewöhnt und sind bereit, mögliche Risiken einzugehen, um im Gegenzug mehr Komfort zu erhalten: Die Software erleichtert schliesslich ihre Aufgabe. Der Ruf eines Unternehmens spielt hierbei eine wichtige Rolle. Je ethischer und glaubwürdiger das Firmenversprechen, umso grösser sind Bereitschaft und Vertrauen, persönliche Informationen zu teilen.

Auch bei AR sind viele Funktionen ohne solche Personendaten nicht umsetzbar. Was diese Lösungen aber einzigartig macht, ist die Kombination aller Daten in einer einzigen Plattform. Diese Aggregation mündet in höherer Genauigkeit und Qualität der gesammelten Daten, zum Beispiel für Gesichtserkennung oder Positionsverfolgung. Im Gegensatz zu anderen Szenarien zeichnen die Sensoren bei AR konstant und in Echtzeit auf und nicht nur punktuell in vorbestimmten Situationen. Weil dabei nicht nur Reaktionen und Aktionen der Nutzer:innen erfasst, sondern auch die auslösenden Situationen und der Kontext festgehalten werden, lassen sich sogar Rückschlüsse auf unbewusstes Verhalten oder passive Handlungen ziehen.

Nicht nur eine Frage der Ethik

Setzt ein Unternehmen AR zur Optimierung der eigenen Prozesse oder als Teil seines Marktangebots ein, nimmt die Pflicht für eine umsichtige Datenverantwortung zu. Wichtig ist, transparent zu kommunizieren, wie der Schutz und die Verwendung von gesammelten Daten gehandhabt werden. So können Befürchtungen reduziert und Vertrauen aufgebaut werden.

Verlässliche und vor allem auch in fernerer Zukunft noch gültige Leitplanken sind dafür nicht auszumachen. Regulatorien und Sicherheitsstandards sind je nach Region in unterschiedlichen Entwicklungsstadien und Ausprägungen präsent. Die weiter steigende Sensibilität für Datenschutz lässt darauf schliessen, dass die öffentliche Meinung noch nicht gefestigt ist. Was heute akzeptiert wird, kann morgen in einem «Shit-storm» enden.

Selbstregulierungsbestrebungen von Organisationen wie XR Safety Initiative (XRSI) oder OpenARCloud fördern die Aufklärung und bieten Best Practices. Ein bewusster und proaktiver Umgang mit Fragen des Schutzes persönlicher Daten ist dabei zentral für die nachhaltige Wirtschaftlichkeit von AR-Lösungen. Es geht darum, die Innovation zuzulassen, aber einen drohenden Reputationsschaden abzuwenden und die Investitionen respektive den Profit daraus zu sichern.

Es empfiehlt sich, als Unternehmen für AR-Projekte auf «Privacy by Design» zu setzen. Dabei wird der Schutz sensitiver Daten bereits in der Konzeptions- und Entwicklungsphase von Anwendungen nicht nur berücksichtigt, sondern gewährleistet. Die gesammelten Daten werden auf das Erlaubte, Notwendige und Sinnvolle reduziert und nicht abgespeichert, sofern sie nur unmittelbar gebraucht werden. Zugriffskontrollen und Verschlüsselung sind zentrale Funktionen: Nur berechtigte Rollen dürfen auf die entsprechenden Daten zugreifen.

Informed Consent

Eine der wichtigsten Massnahmen ist, Transparenz über die aufgezeichneten Daten und deren Verwendung herzustellen. Dies gelingt am besten, indem Nutzer:innen einbezogen werden und selbst mitentscheiden können. Sie sollen die Wahl haben, zugunsten eines für sie vorteilhafteren Risikoprofils auf Funktionen oder Genauigkeit zu verzichten. Je nach Szenario kann dieser «Informed Consent» sogar situationsspezifisch eingeholt werden, im Sinne von: «Darf das Videobild für die nächsten 5 Minuten vom Cloud-Dienst Facial Recognition analysiert werden? Ja/nein – mehr Infos».

Die Vorteile von Augmented Reality

BUSINESS CASE	NUTZEN UND BEISPIELE
AR-NAVIGATION	• EINFACHE ORIENTIERUNG, SEHENSWÜRDIGKEITEN FINDEN • WEGLEITUNG, Z.B. ZUM RESTAURANT ODER IN EINEM GROSSEN GEBÄUDE
ZUSÄTZLICHE INFORMATION ZUR REALEN WELT	• NUTZER:INNENINTENTION ERKENNEN, UM INFORMATIONEN AN DIE SITUATION ANZUPASSEN • SCHNELLERE INTERAKTION MIT OBJEKTEN UND FUNKTIONEN – EINFACHERE, KONTEXTSENSITIVE BEDIENUNG, Z.B. INNENEINRICHTUNG PLANEN • INFORMATIONEN VOR ORT ZUGÄNGLICH MACHEN (LAGERHALTUNG IM RETAIL, WARTUNG UND BETRIEB VON IOT-GERÄTEN)
UNTERHALTUNG	• ORTSABHÄNGIGER, VIRTUELLER INHALT, Z.B. POKÉMON GO • SHARED CONTENT
REMOTE COLLABORATION	• REMOTE COLLABORATION MIT VIRTUELLER PRÄSENZ • DIE EIGENE SICHT TEILEN UND IM TEAM ARBEITEN – AUS SICHERER DISTANZ • SCHNELLE UND KOSTENGÜNSTIGE EXPERT:INNEN-HILFE, Z.B. TELEMEDIZIN ODER WARTUNG UND BETRIEB VON MASCHINEN
SCHULUNG UND TRAINING	• IMMERSIVE INTERAKTION IM VIRTUELLEN RAUM • EXTREMSITUATIONEN KÖNNEN SIMULIERT WERDEN • PERSÖNLICHE ERFAHRUNG VERBESSERT DAS TRAININGSERGEBNIS • PSYCHOLOGISCHES TRAINING, Z.B. ANGSTTRAINING

Risiken in Augmented-Reality-Anwendungen

URSPRUNG	RISIKEN BEI UNGEWÜNSCHTER NUTZUNG VON DATEN
PERSON/CUSTOMER IDENTIFYING DATA (PID/CID)	• GENAUE BEWEGUNGSDATEN • PERSONAL IDENTIFYING / BIOMETRISCHE DATEN – Z.B. SENSITIVE PATIENT:INNENDATEN • FAKE IMPERSONATION – HIJACKING PROFILE UND AVATAR • SOCIAL ENGINEERING – PROFILING UND TARGETING • ATTENTION TARGETING – MANIPULATION VON PERSONEN
RÄUMLICHER KONTEXT	• ÖFFENTLICHER RAUM UND ARBEITSUMFELD • PRIVATER/HALBPRIVATER RAUM MIT PERSÖNLICHEN DETAILS • VERMESSUNG UND AUFNAHME VON ORTEN UND RÄUMEN
SITUATIVER KONTEXT	• UNBEWUSSTES TEILEN VON PRIVATEN ODER GESCHÜTZTEN INHALTEN • SENSITIVE AUFNAHMEN IM BUSINESSUMFELD VON ORTEN, PRODUKTEN, KONVERSATIONEN
UNBETEILIGTE DRITTE	• PERSÖNLICHKEITSRECHTE VON PASSANT:INNEN
VIRTUELLER INHALT	• VERLETZUNG VON URHEBERRECHT • ONLINE HARASSMENT • ABUSIVE CONTENT
CROWD SOURCING	• CONTENT MODERATION • FILTERUNG • URHEBER- UND EIGENTUMSRECHT

Textlastige Zustimmungserklärungen und AGB haben in diesem Zusammenhang nichts verloren. Die Wahrscheinlichkeit, dass Nutzer:innen diese lesen, ist sehr gering. Vorzuziehen sind animiert gestaltete, möglicherweise sogar interaktive Anleitungen und Tutorials im direkten Anwendungskontext. Gleichzeitig publiziert das Unternehmen relevante Richtlinien und «Codes of Conduct» und verpflichtet sich, diese Spielregeln ebenfalls einzuhalten. Heute sind solche Konzepte vor allem in kommunikativen Plattformen und sozialen Medien verbreitet. In Zukunft werden auch andere Anwendungen formulieren, wie die Zusammenarbeit und der Umgang miteinander gesteuert werden.

Auf Stärken fokussieren

Augmented Reality hat die Fähigkeit, das Erlebnis der Nutzer:innen auf das nächste Level zu heben und dadurch entsprechende Markterfolge zu erzielen. Die Risiken, die mit AR einhergehen, sind jedoch vielfältig, insbesondere in Bezug auf Personendaten und in einer längerfristigen Betrachtung. Deshalb ist es notwendig, transparent und verständlich über die Verwendung persönlicher Daten zu informieren und den Nutzer:innen die Entscheidungsfreiheit zu belassen. Die Datensensibilität unserer Gesellschaft wird weiterwachsen. Kritische Hinterfragungen entstehen damit unter Umständen erst, nachdem ein Produkt bereits eingeführt wurde. Um derartigen Veränderungen vorzugreifen oder adäquat darauf zu reagieren, übertragen Unternehmen die Marktbeobachtung an Expert:innen, die nah am Puls sind und Auswirkungen auf Security und Schutz der Privatsphäre schnell einordnen können. />

Lust auf mehr?

Digitalisierungsvorhaben
Zukunftsmacher
Tech-Trends

Jetzt bestellen
ergon.ch/smart2021

