SF·FS

Schweizer Forum für
Kommunikationsrecht

Forum Suisse pour le Droit
de la Communication

CENTER FOR INFORMATION TECHNOLOGY SOCIETY AND LAW — ITSL

ZLSR | Zentrum für Life Sciences-Recht

TECH LAW WORKSHOP
Angriffe auf KI-Systeme

10. November 2023, 13:30 – 18:00 Uhr
FFHS Gleisarena Zürich
Zollstrasse 17
8005 Zürich

TECH LAW WORKSHOP
Angriffe auf KI-Systeme

Der Einsatz von KI-Systemen bringt neue Risiken mit sich. Diskutiert werden hierbei bislang vor allem die (oft auf so genannten Biases beruhende) Diskriminierung von Individuen oder deren gezielte Manipulation. Auch die mangelnde Transparenz der KI-Systeme, insbesondere hinsichtlich Erklärbarkeit und Nachvollziehbarkeit, beschäftigt die Forschung.

Noch weniger präsent ist dagegen die Tatsache, dass diese Systeme auf vielfältige Weise angegriffen und manipuliert werden können, was weit reichende Folgen für deren Sicherheit sowie für die Sicherheit all jener Personen hat, die mit den Systemen interagieren.

Aber welche Gefahren existieren wirklich? Kommt es in der Praxis bereits zu solchen Angriffen? Sind diese Gefahren aus technischer Sicht wirklich neu? Und vor allem: Mit welchen technischen und rechtlichen Regeln lassen sie sich unter Kontrolle bringen? Aufgeworfen ist damit auch die Frage, ob bestehende Normen angepasst oder neue geschaffen werden müssen, um die mit solchen Angriffen einhergehenden Risiken zu kontrollieren.

Diese Fragen werden in einem neuen Workshop-Format im Austausch zwischen Wissenschaft und Praxis aus verschiedenen Perspektiven diskutiert. Neben kurzen Inputs bleibt ausreichend Zeit für eine moderierte offene Diskussion. Die Teilnehmerzahl ist auf 30 Personen begrenzt.

Der «Tech Law Workshop» wird gemeinsam vom Schweizer Forum für Kommunikationsrecht (SF-FS), dem Zentrum für Life Sciences-Recht (ZLSR) der Universität Basel und dem Center for Information Technology, Society, and Law (ITSL) der Universität Zürich organisiert.

PROGRAMM

13:30 – 13:40
Begrüssung und Einführung
Prof. Dr. ALFRED FRÜH, Universität Basel

Teil I: Probleme
13:40 – 14:00
Arten und Vorkommen von Angriffen auf KI-Systeme
Dr. KATHRIN GROSSE, EPFL Lausanne

14:00 – 14:10
(Potenzielle) Schäden
Dr. DARIO HAUX, Zürich

14:10 – 14:30
Diskussion: *Phänomen, Vielfalt, Gefahren, Handlungsbedarf*

Pause

Teil II: Lösungen
15:00 – 15:15
Technische Massnahmen
DOMINIC PIERNOT, IT-Forensiker, Offenburg

15:15 – 15:30
Rechtliche Massnahmen: Strafrecht
COLIN CARTER, MLaw, Universität Basel

15:30 – 15:45
Rechtliche Massnahmen: Haftungsrecht
Prof. Dr. MELINDA LOHMANN, Universität St.Gallen

15:45 – 16:00
Rechtliche Massnahmen: Immaterialgüterrecht
Prof. Dr. ALFRED FRÜH, Universität Basel

Pause

16:15 – max. 18:00
Diskussion: *Wirksamkeit Massnahmen de lege lata, Differenzierungen, Regelungsbedarf, Regelungsumfang, Regelungsebene*

ab 18:00
Apéro riche

ANMELDUNG

Die Anmeldung erfolgt über die Website: **www.sf-fs.ch**

Die **Teilnahmegebühren** betragen
- für Nichtmitglieder: CHF 250.–
- für Mitglieder des SF-FS: CHF 150.–
- Studierende: CHF 50.– (Bitte Legikopie einsenden an **info@sf-fs.ch**)

Sie können Mitglied werden (www.sf-fs.ch/mitgliedschaft) und sofort weniger bezahlen.
Die Anmeldung verpflichtet zur Bezahlung innert 14 Tagen ab Zustellung der Rechnung.

Wir freuen uns auf Ihre Teilnahme.

Artwork: Dall-E

SF•FS
Schweizer Forum für Kommunikationsrecht

Rämistrasse 74 / 56
CH-8001 Zürich

T +41 44 634 42 00

info@sf-fs.ch
www.sf-fs.ch