Digitale Kriminalprävention

Strategien zum besseren Schutz von Minderjährigen im Internet

Thomas-Gabriel Rüdiger
Doktor der Rechtswissenschaften (Dr. jur.), Leiter des Instituts für Cyberkriminologie, Inhaber der Professur für Kriminalistik, Cyberkriminalwissenschaft und Kriminalprävention, Hochschule der Polizei des Landes Brandenburg.

Seit Jahren ist absehbar, dass der digitale Raum gerade für Minderjährige viele Risiken birgt. Bisher ist es allerdings nicht einmal ansatzweise gelungen, effektive Schutzmaßnahmen zu etablieren. Schutzmaßnahmen müssen als vernetzte Aufgabe unterschiedlichster Instanzen wahrgenommen und als Teil einer digitalen Kriminalprävention verstanden werden. Ein vergleichender Blick auf die Verkehrsprävention im öffentlichen Raum könnte dabei lohnend sein. Denn es besteht eine eingeübte gesellschaftliche Praxis, dass Eltern ihre Kinder über die Grundregeln des Verhaltens im Straßenverkehr aufklären. Eine Untersuchung aus dem Jahr 2003 ergab, dass nahezu alle Eltern – insgesamt 98 Prozent – ihren Kindern das richtige Verhalten an Zebrastreifen und das Anhalten am Bordstein beibringen.

Auch Kindergärten und Schulen greifen diese Form der Verkehrsprävention auf, wenn sie mit Kindern Ausflüge unternehmen und mit ihnen einüben, wie sie sich orientiert an Verkehrszeichen zu verhalten haben. Die Vermittlungsarbeit verdeutlicht, dass es staatlich verankerte Regularien gibt, die eine allgemeine – teilweise sogar globale – Gültigkeit erlangt haben. Regeln benötigen bei Normenbrüchen jedoch

auch Sanktionen und eine institutionelle Wahrscheinlichkeit der Durchsetzung. Eine Studie aus Kanada zeigt, dass eine lediglich vermutete Wahrnehmbarkeit von Polizei im Straßenverkehr zur Reduzierung von Normenüberschreitungen führen kann.[1] Gleichzeitig sind Infrastrukturen wie Zebrastreifen und Ampeln vorhanden, die die Grundlage des sicheren Bewegens in diesem Raum bilden. Zwar hat dies alles nicht dazu geführt, dass es zu keinen Unfällen mehr kommt, doch wurde dadurch ein risikominimierter Raum für die Verkehrsteilnehmer geschaffen.

Digitale Bildung durch Eltern und Schulen

Viele Menschen verbringen einen großen Teil ihrer Zeit im „digitalen Verkehrsraum" und werden dort mit einer Vielzahl von Risiken konfrontiert. In Deutschland nutzen bei den 14- bis 59-Jährigen täglich 100 Prozent Online-Angebote, bei den 60- bis 69-Jährigen sind es 96 Prozent.[2] Jugendliche sind im Durchschnitt 71 Stunden online,[3] und 64 Prozent der Sechs- bis Neunjährigen nutzen zumindest gelegentlich ein Smartphone.[4] Während 39 Prozent der Eltern die Smartphonenutzungszeit ihrer Kinder regulieren, verzichten 55 Prozent der Eltern darauf, technische oder andere begleitende Maßnahmen zum Schutz ihrer Kinder vorzunehmen.[5] Dabei sind sich Eltern der Risiken bewusst: Im Rahmen der KIM-Studie, einer Basisuntersuchung zum Medienumgang Sechs- bis Dreizehnjähriger, gaben 80 Prozent der Befragten an, dass das Internet Gefahren für Kinder berge. 79 Prozent der Erziehungsberechtigten wünschen sich Medienkompetenz als Schulfach.[6]

Berücksichtigt werden muss ebenfalls, dass es immer Erziehungsberechtigte geben wird, die nicht bereit oder fähig sind, digitale Bildung zu vermitteln. Es gibt nur eine Institution, die unabhängig von ihrem Elternhaus alle Kinder und Jugendlichen erreicht: die Schule. Zwar existieren in den Bundesländern unterschiedliche Formen der Vermittlung digitaler Bildung und seit 2016 auch eine diesbezügliche Strategie der Kultusministerkonferenz, jedoch belegt die *International Computer and Information Literacy Study* rückläufige Entwicklungen in diesem Bereich. Während die digitalen Kompetenzen von Gymnasiasten in Deutschland seit 2013 weitestgehend stabil geblieben sind, sind sie an anderen Schulformen der Sekundarstufe I im gleichen Zeitraum sogar signifikant um 31 Punkte gesunken; im Jahr 2018 befanden sich 33 Prozent der Achtklässler in den niedrigsten Kompetenzstufen für digitale Fähigkeiten, 2023 waren es hingegen über 40 Prozent.[7] Die Studienleiterin fasste die Ergebnisse in einem Tagesschau-Interview überspitzt so zusammen, dass diese 40 Prozent der Schülerinnen und Schüler „im Grunde genommen nur klicken und wischen" können.[8] Es zeigt sich zudem nicht nur ein Unterschied zwischen den Schulformen, sondern auch zwischen den

1 Rylan Simpson et al.: „Reducing speeding via inanimate police presence", in: Criminology & Public Policy, 19. Jg., Nr. 3/2020, S. 997-1018, DOI: 10.1111/1745-9133.12513.

2 ARD/ZDF-Forschungskommission: ARD/ZDF-Medienstudie 2024: Mediennutzung in Deutschland. Basispräsentation.

3 Postbank: Jugend-Digitalstudie 2024: Jugendliche sind wieder mehr online – auch für Schule, Ausbildung oder Studium. Medieninformation, 30.10.2024.

4 Bitkom: Kinder & Jugendliche verbringen täglich zwei Stunden am Smartphone, Presseinformation, Berlin, 06.08.2024.

5 Sabine Feierabend et al.: KIM 2024. Kindheit, Internet, Medien – Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland, hrsg. v. Medienpädagogischen Forschungsverbund Südwest (mpfs).

6 Sabine Feierabend et al.: KIM 2022. Kindheit, Internet, Medien – Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland, hrsg. v. Medienpädagogischen Forschungsverbund Südwest (mpfs).

7 Birgit Eickelmann et al.: ICILS 2023 #Deutschland. Computer- und informationsbezogene Kompetenzen und Kompetenzen im Bereich Computational Thinking von Schüler*innen im internationalen Vergleich, Waxmann Verlag, Münster / New York 2024.

8 Tagesschau: „40 Prozent der Achtklässler laut Studie nicht fit am PC", in: tagesschau.de, 12.11.2024.

Bundesländern. Laut Bildungsmonitor nehmen die ostdeutschen Bundesländer bei der Digitalisierung seit Jahren die hinteren Plätze ein.[9]

Die Vorbereitung auf die Risiken des Zeitalters der Künstlichen Intelligenz (KI) darf allerdings nicht davon abhängig sein, ob ein Kind zufällig die „richtige" Schule im „richtigen" Bundesland besucht. Die Frage, ab wann digitale Bildung vermittelt werden sollte, muss sich an den bereits dargestellten Medienzahlen orientieren: Einige Kinder erhalten bereits ab der ersten Klasse und sogar früher Zugang zum globalen und relativ ungesicherten digitalen Raum, obwohl digitale Bildung beziehungsweise die Vermittlung von Medienkompetenz institutionell meist erst an weiterführenden Schulen diskutiert wird. Eine verpflichtende Vermittlung digitaler Bildung ab der ersten Klasse findet nicht statt. Dies mag vielleicht auch daran liegen, dass die digitale Bildung von den vorhandenen Lehrkräften geleistet werden müsste. Fast die Hälfte der befragten Schüler verneint aber, dass die Lehrkräfte an ihrer Schule über die erforderlichen Kompetenzen verfügen würden, um digitale Geräte im Unterricht zu nutzen.[10]

Entwicklung im KI-Bereich erfordert mehr Kriminalprävention

Digitale Bildung sollte auch als ein notwendiger Teil einer grundlegenden digitalen Kriminalprävention verstanden werden.[11] Im besten Fall bedeutet die Vermittlung digitaler Kompetenzen nicht nur, dass Minderjährige weniger mit Kriminalität konfrontiert werden, sondern auch, dass sie über rechtliche Fragen so aufgeklärt werden, dass sie selbst als Tatverdächtige weniger in Erscheinung treten. Beides ist notwendig. Knapp 60 Prozent der Jugendlichen berichten, dass sie monatlich mit Fake News konfrontiert werden, 57 Prozent mit beleidigenden Kommentaren, 54 Prozent mit extremen politischen Ansichten, 40 Prozent mit Hassbotschaften und 25 Prozent mit pornografischen Inhalten.[12] Beunruhigende 16 Prozent der unter 14-jährigen Kinder und 24 Prozent der befragten Minderjährigen waren bereits von Cybergrooming betroffen,[13] sodass dieser Straftatbestand leider als eine Art Normalität im digitalen Raum gelten muss. Entsprechend wünschen sich zwei Drittel der Minderjährigen mehr schulische Aufklärung zu diesem Phänomen.[14] Gleichzeitig machen Minderjährige bei digitalen Sexualdelikten seit einiger Zeit selbst einen signifikanten Anteil der Tatverdächtigen aus.[15]

Zudem zeichnet sich durch die Entwicklungen im KI-Bereich eine Verschärfung der Situation ab. Fälle, in denen mithilfe einfacher Apps Nacktbilder von Mitschülern oder fremden Personen angefertigt werden, häufen sich international. Gleichzeitig treten sogenannte KI-Agenten – Softwareprogramme, die Künstliche Intelligenz nutzen,

9 Institut für Soziale Marktwirtschaft (INSM): Bildungsmonitor 2024, letzte Aktualisierung 07.07.2025.

10 Doris Lewalter et al.: PISA 2022, Waxmann Verlag, Münster / New York 2023.

11 Thomas-Gabriel Rüdiger: „Digitale Bildung als Eckpfeiler einer digitalen Kriminalprävention", in: Erziehung und Unterricht - Österreichische Pädagogische Zeitschrift, 175. Jg., Nr. 5-6/2025, S. 408-419.

12 Sabine Feierabend et al.: JIM 2024. Jugend, Information, Medien. Basisuntersuchung zum Medienumgang 12- bis 19-Jähriger in Deutschland, hrsg. v. Medienpädagogischen Forschungsverbund Südwest (mpfs).

13 Sabrina Nennstiel / Meike Isenberg: Kinder und Jugendliche als Opfer von Cybergrooming. Zentrale Ergebnisse der 5. Befragungswelle 2025, Landesanstalt für Medien NRW, Düsseldorf 2025.

14 Ebd.

15 Thomas-Gabriel Rüdiger et al.: „Phänomenologie und Präventionsansätze bei digitalen Sexualdelikten durch minderjährige Tatverdächtige", in: Rita Steffes-enn (Hrsg.): Sexueller Kindesmissbrauch und Missbrauchsabbildungen in digitalen Medien, Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin 2023, S. 225-235.

um selbstständig Aufgaben zu erledigen und eigene „Ziele“ zu verfolgen – als Risiko für Minderjährige in Erscheinung.

Ein Fall aus Florida hat großes Aufsehen erregt: Ein 14-jähriger Junge soll sich im Jahr 2024 in einen KI-Chatbot verliebt haben. Nach einiger Zeit soll der Jugendliche suizidale Gedanken geäußert haben, wobei er offenbar wiederum teilweise durch den Chatbot dazu motiviert wurde. Nach dem tragischen Selbstmord des Jungen verklagte die Mutter die KI-Anbieter wegen mangelnden Kinderschutzes.[16] Der Vorfall deutet auf eine Zukunft hin, in der Kinder mit als menschlich wahrgenommenen Formen von KI und humanoiden Robotern aufwachsen und diese im Extremfall als Freunde oder gar Liebespartner wahrnehmen. Er wirft auch die Frage auf, welche Kriminalitätsformen aus dieser neuen Situation erwachsen.

Mehr Sichtbarkeit der Sicherheitsbehörden im Netz

Ähnliche digitale Risiken lassen sich auch für Erwachsene belegen. Zu erwarten ist, dass die Besonderheiten des digitalen Raums zu deutlich höheren Kriminalitätsraten führen als im analogen. Es ist daher zu fragen, welche Funktion die Sicherheitsbehörden im Vergleich etwa zum Straßenverkehr einnehmen, um einen sicheren digitalen Raum zu gewährleisten. Im Straßenverkehr sind Sichtbarkeit und Ansprechbarkeit der Ordnungskräfte wichtig für die Durchsetzung des staatlichen Gewaltmonopols. Erst durch Uniformen, Streifenwagen oder Wachen werden Polizei und Ordnungsamt für die Bürgerinnen und Bürger erkenn- und ansprechbar. Potenziellen Tätern wird signalisiert, dass der Staat sein Gewaltmonopol wahrnimmt, und er führt ihnen das Entdeckungsrisiko vor Augen. Diese Mechanismen fehlen weitgehend im Internet, was zunehmend als Defizit erkannt wird. Demzufolge sprach der Präsident des Bundeskriminalamtes (BKA) davon, „dass für junge Menschen es heute völlig normal ist, dass Kriminalität im digitalen Raum stattfindet, so werden sie groß“, und weiter: „Sie sehen Polizei aktiv werden, wenn wir draußen kontrollieren, im Netz nehmen wir das gar nicht wahr.“[17]

Die Sicherheitsbehörden sind im digitalen Raum nur eingeschränkt sicht- und wahrnehmbar. Ihre Präsenz konzentriert sich zum einen auf sechzehn Internetwachen, bei denen zudem keine direkte Interaktion mit den Bürgern möglich ist – sie ähneln eher digitalen Briefkästen –, zum anderen auf Social-Media-Accounts, auf denen nicht selten Hinweise wie „Hier keine Anzeigen“ oder „Nachrichten werden nicht gelesen“ zu finden sind.[18] Formen zufälliger und wahrnehmbarer virtueller Polizeistreifen, die auch proaktiv nach Straftaten suchen, sind von den Usern faktisch nicht feststellbar. Es fehlt an individuellen und nutzerfreundlichen digitalen Kommunikationsangeboten zur Polizei,

16 „US-Bundesgericht in Florida: Mutter verklagt KI-Firma und Google wegen Suizids ihres Sohnes“, in: Der Spiegel, 24.10.2024.

17 Unabhängige Beauftragte für Fragen des sexuellen Kindesmissbrauchs (UBSKM): Pressekonferenz zur Polizeilichen Kriminalstatistik 2022 - Zahlen kindlicher Gewaltopfer, hrsg. v. USBKM und BKA.

18 Thomas-Gabriel Rüdiger: „Digitale Polizeipräsenz - Die kriminalpräventive Funktion digitaler Polizeipräsenz zwischen virtuellen Polizeistreifen und Kinder-Online-Wachen“, in: SIAK-Journal, Nr. 4/2023, S. 40-61.

vor allem für Kinder. Wenn sie etwas Problematisches erleben, könnten sie bei einem derartigen Angebot beispielsweise per Knopfdruck direkt einen Videochat mit der Polizei führen. Eine Art Kinderonlinewache, die rund um die Uhr digital erreichbar wäre, könnte vermitteln, dass die Polizei – egal, was Kinder im digitalen Raum erleben – für sie online ansprechbar ist.[19]

Zurzeit setzen die Menschen bei Anzeigen von Delikten im digitalen Raum kaum auf die Polizei. So ergab eine Studie, dass die Bereitschaft junger Menschen, Formen digitaler Hasskriminalität bei der Polizei anzuzeigen, von einem Prozent im Jahr 2022 sogar auf null im Jahr 2023 gesunken ist. Hingegen stieg die Bereitschaft, dies bei den Portalen zu melden, auf 30 Prozent.[20] Das heißt: Die Sicherheitsbehörden werden teilweise nicht mehr als Akteure zur Bekämpfung digitaler Kriminalität wahrgenommen; vielmehr wird dies auf Betreiber, zivile Meldestellen und andere Akteure ausgelagert. Generell ist auch deshalb die Wahrscheinlichkeit einer Strafverfolgung bei digitalen Delikten wesentlich niedriger als bei analogen.[21] Selbst Beamte des Bundeskriminalamtes räumen ein,[22] dass der digitale Raum von den Sicherheitsbehörden nicht genauso wie der analoge Raum bei der Bekämpfung digitaler Sexualdelikte durchdrungen wird. Dies gilt besonders im Hinblick auf das Ziel, diesen Raum für Minderjährige sicherer zu machen.

Virtuelle Polizeistreifen

Schließlich stellt sich die Frage, inwiefern Politik und Internetfirmen für eine sichere digitale Infrastruktur für Kinder sorgen müssten, die mit einer Art digitalem Bürgersteig oder einer Ampel vergleichbar wäre. Hier kommen viele grundlegende Fragen in Betracht: Warum müssen Moderatoren in sozialen Medien und vor allem in Onlinespielen nicht ähnlich wie Mitarbeiter von Sicherheitsfirmen staatlich geprüft und zertifiziert werden? Warum sind die Altersfreigaben der Unterhaltungssoftware Selbstkontrolle (USK) für digitale Spiele und Apps nicht auch an Kommunikationsrisiken gekoppelt, sodass eine Altersfreigabe ab 0, 6 oder 12 Jahren auch bedeutet, dass in diesem Spiel keine fremde Person unkontrolliert mit dem Kind kommunizieren kann und es entsprechende Schutzmaßnahmen gibt? Warum gibt es noch immer keinen wirksamen Einsatz von Systemen zur Altersverifikation, damit Kinder sich nicht in den Programmen – auch gegen deren eigene Geschäftsbedingungen – anmelden können? Warum sind die Regularien zum Schutz von Kindern im digitalen Raum noch immer zwischen Bund (Jugendschutzgesetz) und Ländern (Jugendmedienschutzstaatsverträge) aufgeteilt? Aktuell lässt sich behaupten, dass weder die Politik noch die Betreiber Minderjährige effektiv vor digitalen Risiken schützen.

19 Thomas-Gabriel Rüdiger, a. a. O., siehe Rn. 18.

20 Sabrina Nennstiel / Meike Isenberg: Hate Speech - Forsa-Studie 2023. Zentrale Untersuchungsergebnisse, Landesanstalt für Medien NRW, Düsseldorf 2023.

21 Thomas-Gabriel Rüdiger, a. a. O., siehe Rn. 18.

22 STRG_F (2024): Pädokriminelle im Stream: So sicher fühlen sich Täter. Siehe auch die gleichnamige ZDF-Dokumentation, 12.06.2024.

Eine wirksame digitale Kriminalprävention erfordert ein komplexes Ineinandergreifen unterschiedlicher Akteure und Institutionen, vergleichbar mit der Verkehrsprävention. Notwendig ist die Vermittlung digitaler Bildung für alle Altersstufen – eventuell in Form eines digitalen Führerscheins –, damit Erwachsene in der Lage sind, Minderjährige auf diesen Bereich vorzubereiten und ihnen digitale Ethik zu vermitteln. Darüber hinaus ist eine verpflichtende institutionelle Vermittlung digitaler Bildung an alle Schüler ab der ersten Klasse notwendig. Dies erfordert die Bereitstellung entsprechender personeller, finanzieller und, falls Lehrkräfte dafür eingesetzt werden, auch zeitlicher Ressourcen.

Gleichzeitig müssen Sicherheitsbehörden dem digitalen Raum genauso viel Priorität zumessen wie dem analogen. Das bedeutet, dass die Wahrscheinlichkeit, dass Täter im sogenannten *Clearweb* strafrechtlich verfolgt werden, signifikant gesteigert wird. Die Gesellschaft sollte auch verstärkt über virtuelle Polizeistreifen, die selbst aktiv nach Straftaten im digitalen Raum suchen, diskutieren – die Polizei in Nordrhein-Westfalen nimmt in diesem Bereich derzeit eine Vorreiterrolle ein. Zudem sollten die Anzeige- und Kommunikationsmöglichkeiten im digitalen Raum für alle Altersstufen so einfach wie möglich gestaltet werden, was eine zentrale Internetwache für ganz Deutschland sowie spezielle Angebote, wie eine Kinderonlinewache, erfordert.

Dazu ist ein entsprechender politischer Wille notwendig, wirklich etwas an der gegenwärtigen Lage zu ändern. Die Politik muss einerseits eine digitale Infrastruktur zur Kriminalitätsbekämpfung im Netz schaffen und auch die Problematik föderativer Strukturen in einem globalisierten Raum thematisieren. Andererseits muss sie die Betreiber dazu verpflichten, wirksame Schutzmaßnahmen für Minderjährige zu integrieren. Bisherige Annahmen, dass beispielsweise eine freiwillige Selbstkontrolle wirksam sein könnte, haben sich weitgehend als Illusion erwiesen. Nicht umsonst unterstützt sogar *Meta* inzwischen eine verpflichtende Altersfreigabe als „digitale Volljährigkeit" ab sechzehn Jahren für alle sozialen Medien und deren Überprüfung. Dies zeigt, dass selbst globale Player den bisherigen Schutz als nicht wirksam einstufen.[23] Eine entsprechende Altersbeschränkung würde aus kriminalpräventiver Sicht einen gewissen Sinn ergeben. Das darf jedoch nicht dazu führen, dass die Vermittlung digitaler Bildung zurückgenommen wird. Es muss beides geben: Verbote von Social-Media-Programmen für Kinder und die Vermittlung digitaler Bildung.

23 Malte Kirchner: „Meta unterstützt Idee einer EU-weiten digitalen Volljährigkeit", in: heise online, 04.07.2025.

Die Internetlinks zu den Quellen sind in der Onlinefassung des Beitrags enthalten, abrufbar unter *www.kas.de/de/web/die-politische-meinung/artikel/detail/-/content/digitale-kriminalpraevention.*