Der „Smart-Ort“ als Tatort

– wie neue digitale Spuren die Ermittlungsarbeit verändern

Von KOR Alexander Hahn, Kiel1

Digitale Spuren machen im Zeitalter der digitalen Geräte bzw. der digitalen Kommunikation einen nicht unwesentlichen Anteil aller Ermittlungsansätze aus – oftmals sind sie sogar die einzigen Ermittlungsansätze. Diese Thematik wird künftig weiter an Bedeutung gewinnen, da immer mehr Menschen mit immer mehr Geräten immer mehr digital kommunizieren werden. Bestes Beispiel ist das sogenannte *„Internet der Dinge“*: Zunehmend mehr Haushaltsgeräte und andere Alltagsgegenstände werden dabei an das Internet oder andere Netzwerke angeschlossen.

Auch Fahrzeuge oder sogar Heizungsanlagen dürften künftig vermehrt über einen eigenen Internetzugang verfügen. Sicher ist, dass auf diesem Weg enorme Mengen an digitalen Spuren erzeugt werden. Auch wenn Kommunikationsspuren von Heizungsanlagen eher selten zur Lösung eines Falles beitragen dürften, lässt sich zumindest erahnen, welche Bedeutung digitale Spuren in Fahrzeugen haben werden. Digitale Spuren in Computern und Smartphones sowie in Funkzellen gehören dabei zwar zum Thema, sind aber bereits ein „alter Hut“. Dieser Artikel beschäftigt sich mit neuartigen digitalen Spuren, die zukünftig überall sein werden – und von denen wir heute zum Teil noch gar nichts ahnen.

1 Digitale Spuren in Fahrzeugen

Über das Vorhandensein von digitalen Spuren in modernen Fahrzeugen besteht bereits ein gewisses Bewusstsein. Viel zu selten stehen sie aber im Rahmen der polizeilichen Arbeit zur Verfügung.

1.1 Verkehrsunfallermittlungen

Zumindest diejenigen Polizeibeamtinnen und -beamten, deren Ausbildung schon etwas länger zurückliegt, erinnern sich sicherlich noch an eine großartige kriminaltechnische Spurensicherungsidee: Wie kann man bei einem Verkehrsunfall nachweisen, ob ein unfallbeteiligtes Fahrzeug das Licht eingeschaltet, den Blinker gesetzt oder die Bremse getreten hatte? Zur Klärung dieser Frage wurde der Glühfaden in der relevanten Glühbirne unter dem Mikroskop kriminaltechnisch analysiert. Dem

lag, kurz gesagt, die Idee zugrunde, dass der eingeschaltete Glühfaden heiß und biegsam ist und sich in diesem Zustand im Moment des Aufpralls durch den *„Ruck“* charakteristisch verformt. Diese Idee funktioniert bei der Beleuchtung in heutigen Autos mit Xenon- oder LED-Licht allerdings nicht mehr. In diesen Fahrzeugen sind an den wesentlichen Stellen schon lange keine Glühbirnen mehr verbaut, sondern vielmehr computergesteuerte elektronische Leuchtmittel ohne Glühfaden.
Die Frage, ob ein Wagen das Licht eingeschaltet hatte, kann bei Ermittlungen aber eine wesentliche Rolle spielen. Vielleicht stellt aber auch der Beschuldigte in einem (Unfall-)Ermittlungsverfahren einen entsprechenden Beweisantrag oder der Staatsanwalt beauftragt die Polizei mit einer kriminaltechnischen Prüfung dieser Frage. Dafür gilt es, hinsichtlich der Frage *„Licht an oder aus?“* elektronische Spuren im Computersystem eines modernen Autos zu finden. Nicht jede Polizei hat heutzutage selbst die Möglichkeiten für eine solche Prüfung, sondern beauftragt dafür in Einzelfällen entsprechende Gutachter.

1.2 Standortermittlung und Kriminalitätsbekämpfung

Auch bei der Verfolgung von Straftaten dürften digitale Spuren in und von Fahrzeugen eine immer größere Bedeutung erlangen. Die Tatsache, dass Hersteller künftig zwingend Mobilfunk- und GPS-Module in Kombination mit Crash-Sensoren verbauen müssen, um auf diesem Weg automatisch einen Notruf auslösen zu können, eröffnet dem kreativen Kriminalisten ganz neue Möglichkeiten zur Standortbestimmung eines Fahrzeugs. Denkbar ist aber auch eine Telekommunikationsüberwachung in Bezug auf eine fest im Fahrzeug verbaute SIM-Karte, um auf diesem Weg an Daten zu gelangen, die durch mobiles Surfen (Hotspot im Wagen) oder durch das Navigationsgerät (z.B. Verkehrsinformationen) erzeugt worden sind. Derartige Daten können möglicherweise sogar retrograd bei Fahrzeugherstellern oder Drittanbietern abgefragt werden – Erfahrungen oder Standards sind dabei bislang allerdings Mangelware.

1.3 Kraftfahrzeuge als Tatmittel

Telematik-**2** und andere digitale Fahrzeugdaten dürften zukünftig nicht nur bei der Ermittlung von Unfallursachen eine Rolle spielen, sondern auch bei der Aufklärung von Straftaten helfen, bei denen Fahrzeuge als Tatmittel genutzt werden. Einerseits könnten Daten von Sitzdruck- oder Gurtschloss-Sensoren Hinweise auf die Anzahl von Tätern in einem Fahrzeug geben. Andererseits kann die Analyse der Multimedia- bzw. Infotainment-Komponenten in einem modernen Fahrzeug Hinweise auf mit der Fahrzeugelektronik gekoppelte Geräte oder sogar auf Daten geben, die aus Smartphones mit dem Fahrzeug synchronisiert wurden.

1.4 Auswirkungen in Zusammenhang mit Fahrzeugen

Es scheint lohnenswert, gerade die Frage nach digitalen Spuren in Fahrzeugen stärker in den Fokus zu rücken, weil
gesicherte Erkenntnisse bestehen, dass Fahrzeuge eine Vielzahl von digitalen Spuren enthalten
es sich bei Fahrzeugen um eine klar abgrenzbare Art von *„neuen digitalen Dingen“* handelt
bei dieser Art von *„digitalen Dingen“* am ehesten mit standardisiert abgreifbaren digitalen Informationen zu rechnen ist.

In Anbetracht der Tatsache, dass derartige digitale Spuren in Fahrzeugen zukünftig in vielerlei Konstellationen wichtig sein werden und die Extraktion sowie Interpretation selbiger sich sogar zur Standardmaßnahme entwickeln könnte, scheint eines klar: **Die Polizei muss zukünftig selbst in der Lage sein, die Fahrzeugelektronik hinsichtlich derartiger Spuren zu durchsuchen.**

2 Ermittlungen mithilfe von WLAN3-Strukturen

An immer mehr Orten stehen dem Bürger (aber auch dem Straftäter) öffentliche und/ oder freie WLAN-Hotspots zur Verfügung, über die unterschiedlichste Kommunikation erfolgen kann, was wiederum eine Vielzahl von digitalen Spuren erzeugt. Abgesehen davon, dass diese Entwicklung sicherheitspolitisch zumindest bedenklich ist, da sie (vermeintlich) schwierigere Anonymisierungstechniken wie z.B. das Tor-Netzwerk**4** oder VPN-Dienstleister**5** überflüssig erscheinen lässt, müssen sich die Strafverfolger auch über die Ermittlungsmöglichkeiten in diesen Netzen im Klaren sein.

2.1 Flucht ins WLAN

Bereits heute sind Fälle zu beobachten, in denen Täter-Smartphones durch unterschiedliche Funkzellen verfolgt werden konnten und dann aus den eigentlichen Tatortfunkzellen verschwanden, da aufgrund einer Hotspot-Nutzung keine mobilen Telefondienste mehr in der Funkzelle erzeugt wurden. Digitale Spuren finden sich dann nicht mehr in der Funkzelle, sondern lediglich im örtlichen WLAN.

2.2 Spuren im WLAN

Anders als im Fahrzeugbereich ist eine Standardisierung der Spuren hier weit weniger ausgeprägt. So reagieren unterschiedliche Smartphones in Abhängigkeit von ihrer Konfiguration auch unterschiedlich auf vorhandene WLAN-Netze und legen evtl. Spuren eines solchen WLANs in ihrem System ab. WLAN-Router wiederum können Geräte wie z.B. Smartphones mit eingeschaltetem WLAN in ihrer Reichweite registrieren und u.a. die jeweilige MAC-Adresse**6** abspeichern. Oder sie tun es eben nicht. Oder dies passiert nur, wenn sich ein Gerät wirklich mit dem WLAN verbindet. Oder es reicht bei beiden Gerätearten bereits das bloße Registrieren des jeweils anderen aus. Hersteller, Techniken, Systeme und Konfigurationen können hier vielfältig sein und es wird häufig eine Untersuchung des Einzelfalls notwendig sein. Fest steht, dass auf diesem Weg unter Umständen die Anwesenheit eines Smartphones in einem bestimmten WLAN-Bereich (kleine Ausdehnung) nachgewiesen werden kann. Im Idealfall gelingt es so, einen bekannten Tatverdächtigen näher an einen Tatort heranzubringen als bei der Funkzellenabfrage (große Ausdehnung).

2.4 Auswirkungen in Zusammenhang mit WLANs

Ähnlich wie nach einer Tat potenzielle Videoüberwachungen gesucht sowie Funkzellenabfragen durchgeführt werden, dürften zukünftig die am Tatort oder auf dem Fluchtweg liegenden WLANs im Rahmen der Tatortarbeit standardmäßig zu ermitteln sein. Es schließen sich vielfältige Ermittlungsmöglichkeiten an.

3 Ermittlungen in einer „smarten“ Welt

Immer mehr Dinge werden *„smart“* und an das Internet angeschlossen. Die Schlagworte lauten hier *„Internet der Dinge“* und *„Smart-Home“*. Dazu gehört jegliche Alltagstechnik, wie z.B. Telefone, Fernseher, Alarmanlagen, Überwachungskameras, Schließmechanismen, Heizungen, Markisen, Kühlschränke, Ampelanlagen und vieles mehr. In all diesen Geräten können für ein Strafverfahren essentielle digitale Spuren enthalten sein.
Viele *„smarte Dinge“* in einem modernen Haushalt können z.B. die Rückkehr eines Wohnungsinhabers dokumentieren. Alarmanlagen werden aus-, andere Geräte werden eingeschaltet und Verbräuche steigen an. Die dadurch erzeugten Spuren können ebenfalls im Rahmen einer Alibiüberprüfung herangezogen werden. Andererseits kann der findige User bereits heute viele Smart-Home-Technologien beispielsweise über sein Smartphone fernsteuern und so bei tatsächlicher Abwesenheit unter Umständen eine Anwesenheit und damit ein Alibi vortäuschen. Das Themenfeld der *„digitalen Dinge“* ist derart vielschichtig und dynamisch, dass an dieser Stelle auf eine weitere Beschreibung verzichtet wird.

4 Bedeutung der neuen digitalen Spuren für die Polizei

Es erscheint unmöglich, sich der heutigen Digitalisierung der Welt zu entziehen. Digitale Spuren gibt es daher überall.

4.1 Omnipräsenz neuer digitaler Spuren

Neuartige digitale Spuren betreffen nicht nur die *„digitale Kriminalität“* und *„Cybercrime“*. Sie können auch bei der Aufklärung ganz *„weltlicher Ereignisse“* entscheidend sein, z.B. bei Unfällen. Aber auch bei *„analogen Verbrechen“* wie Mordfällen werden zwangsläufig Spuren in der digitalen Welt erzeugt. Dabei verhält es sich ganz ähnlich wie mit der DNA**8**: Digitale Spuren hinterlässt der Täter auf jeden Fall – ob er will oder nicht. Es ist heutzutage nahezu unmöglich, digitale Spuren im engeren oder weiteren Tatortbereich bzw. vor, während oder nach der Tat *nicht* zu hinterlassen. Ähnlich wie bei der DNA ist es dann aber auch mit dem Auffinden dieser neuen Spuren: Sie sind nicht immer auf den ersten Blick zu erkennen. Die Polizei muss daher in

Abhängigkeit von der Bedeutung des Falles schon bei der Tatortarbeit hinreichend viel Zeit und Energie investieren, um digitale Spuren zu identifizieren. Der Aufwand kann sich dabei ganz ähnlich entwickeln wie bei der Suche nach DNA-Spuren am Tatort eines Tötungsdeliktes.

4.2 Spurenschutz

Der *„Smart-Ort“* als Tatort wird die Polizei zukünftig fordern. Gleichzeitig muss sich die Polizei darüber bewusst sein, dass jeder Tatort zugleich auch ein *„Smart-Ort“* ist, an dem digitale Spuren genauso wie herkömmliche Spuren gefunden und gesichert, aber schlimmstenfalls im Rahmen der Tatortarbeit auch zerstört werden können. Fest steht, dass alle Polizeibeamtinnen und Polizeibeamten, egal ob von der Schutz- oder der Kriminalpolizei, an Tatorten mit diesen Spuren konfrontiert sein können. In dieser Situation ist es wichtig, dass man sich über das mögliche Vorhandensein dieser Spuren bewusst ist, dass man im Idealfall diese Spurenarten erkennt und dass man diese Spuren darüber hinaus auch schützt. Diese Erkenntnis führt beispielsweise zu der Frage, ob ein Tatort heutzutage überhaupt noch mit einem eingeschalteten Smartphone betreten werden darf. Schlimmstenfalls können dadurch die z.B. in einem Ringspeicher eines Routers vorhandenen Spuren eines tatrelevanten Smartphones unwiederbringlich überschrieben werden.

4.3 Bedeutung für die Vernehmungstaktik

Das Wissen um die Entstehung bzw. das Vorhandensein digitaler Spuren ist auch in Hinblick auf die Vernehmungsführung unerlässlich. Beispielsweise wird im Rahmen von regelmäßig sehr frühzeitig und z.T. mit relativ wenig Sachverhaltskenntnis durchgeführten Festlegevernehmungen versucht, bei Zeugen und Tatverdächtigen Antworten zu provozieren, die anhand von Fakten überprüft werden können. Dies soll eine Überprüfung der Glaubwürdigkeit einer Aussage ermöglichen. Diese zu überprüfenden Fakten können auch neuartige digitale Spuren sein. Der Vernehmungsbeamte muss sich also über die Entstehungsmöglichkeiten dieser Spurenarten im Klaren sein und kann erst dadurch die richtigen Fragen stellen. *„Welche Geräte haben Sie am Tatort / auf Ihrem Weg / bei sich zuhause genutzt bzw. wann eingeschaltet?“* wäre beispielsweise ein entsprechende Frage, die heutzutage zumindest noch nicht bei jeder derartigen Vernehmung gestellt wird. Wer keine Fragen in Bezug auf neue digitale Spuren stellt, vergibt einen bunten Strauß an Chancen, eine Aussage hinsichtlich ihres Wahrheitsgehaltes überprüfen zu können.

4.4 Probleme durch rasante Entwicklungen

Notebooks, Tablets und Handys sind im Bereich der digitalen Spuren *„Old-School“*. Die Polizei ist hinsichtlich dieser Geräte schon relativ gut aufgestellt, obwohl der ständige Wandel auch in diesem Bereich eine permanente Herausforderung bleibt. Neue digitale Spurenarten werden allerdings schneller entdeckt, als sich Polizeibeamtinnen und -beamte, die ein halbes Leben lang in unterschiedlichsten Bereichen bei der Polizei arbeiten, darauf einstellen können. Der Fortbildung kommt in diesem Themenfeld also nicht nur für die Spezialistinnen und Spezialisten eine enorme Bedeutung zu.

4.5 „Digitale Tatortteams“

Natürlich verfügt die Polizei bereits über gut aufgestellte IT-Beweissicherungseinheiten, die auch mal vor Ort Sicherungen von Computern oder Smartphones durchführen können. Notwendig ist aber eine ausreichende Qualifikation aller Beamtinnen und Beamten in diesem speziellen Themenfeld der neuen digitalen Spuren. Sollte dies allerdings nicht oder nur mit

unverhältnismäßig hohem Aufwand erreicht werden können, so ist es notwendig, den erforderlichen Sachverstand z.B. in Form eines *„digitalen Tatortteams“* auch schon im Rahmen des Ersten Angriffs**9** und möglicherweise als Standardmaßnahme an den Tatort zu bringen. Dieses Team betrachtet den Tatort aus dem *„digitalen Blickwinkel“* und tritt parallel zur *„klassischen“* Spurensicherung in Erscheinung. Dies kann im Extremfall zu der Problematik führen, dass eine Priorisierung der Spurensuche und -sicherung erfolgen muss (herkömmliche Spuren vs. digitale Spuren). Viele Ermittler, die bei einfacher und mittlerer Kriminalität gleichzeitig für die Sicherung althergebrachter Spuren an einem Tatort verantwortlich sind, fühlen Unsicherheit, wenn sie nun auch noch mit der Aufnahme des *„digitalen Tatorts“* betraut werden.

5 Fazit

Die Polizei wird sich der Herausforderung durch immer neue digitale Spuren stellen müssen. Auf Bundesebene existier(t)en diesbezüglich bereits erste Gremien (z.B. AG Embedded Systems/Kfz-Systeme, PG Mikrocontroller). Weiterhin ist bei den Ermittlern innerhalb der Polizei eine entsprechende Sensibilisierung zu beobachten. Bei dieser Thematik spielen darüber hinaus auch rechtliche Aspekte eine wesentliche Rolle. In diesem Beitrag wurde allerdings bewusst auf dieses Themenfeld verzichtet. Für die Taktik und für das Recht wird es künftig eine ewige Herausforderung bleiben, mit der Entwicklung der Technik angemessen Schritt zu halten.

Anmerkungen

1. KOR Alexander Hahn ist Leiter des Dezernates 23 (Cybercrime/digitale Spuren) im LKA Schleswig-Holstein. Daneben nimmt er einen Lehrauftrag im Fachbereich Polizei der FHVD wahr.
2. Gemeint sind ausgetauschte bzw. gespeicherte Daten aus unterschiedlichen Fahrzeugsensoren wie z.B. Geschwindigkeitsverläufe, Bremsbetätigungen, Status des Sicherheitsgurtes etc.
3. Wireless Local Area Network – drahtloses lokales Netzwerk, das regelmäßig auf Basis des Funkstandards der IEEE-802.11-Familie erzeugt wird.
4. Ein auf der Idee des Onion-Routings bestehendes Netzwerk zur Anonymisierung der Teilnehmer.
5. Virtual Private Network – in diesem Fall ein Netzwerk, bei dem die Kommunikation zum Zwecke der Anonymisierung über mindestens einen weiteren Rechner geleitet wird.
6. Individuelle Hardware-Adresse eines Netzwerkadapters innerhalb eines Netzwerkes, die der eindeutigen Adressierung bzw. Identifizierung des Gerätes dient.
7. Dauer der zusammenhängenden Nutzung eines WLANs bzw. des Aufenthaltes im WLAN.
8. DNA-Analysen können mittlerweile mithilfe einer einzigen (!) Körperzelle gelingen.
9. Hier insbesondere Tätigkeiten des Sicherungsangriffs – Versäumnisse im Rahmen des Ersten Angriffs sind auch in diesem Themenfeld kaum nachzuholen.