

23.08.2022

Kleine Anfrage 358

der Abgeordneten Angela Freimuth und Marc Lürbke FDP

Was unternimmt die Landesregierung gegen Identitätsdiebstahl?

Die Identität ist eine den Bewertungszusammenhang betreffende, insoweit flexible Summe aus persönlichen Merkmalen, die eine interaktive Person ausmachen. Dabei kann es sich um eine fragmentierte Person handeln, die nur durch wenige Eigenschaften bestimmt ist (Kontoinhaber, Nickname und Avatar in einer Spiel- oder Kommunikationsumgebung), bis hin zu einem existierenden Menschen in einer vollständigen gesellschaftlichen Umgebung mit ihren diversen Schnittstellen (Melderegister, Sozialversicherungsnummer, Bankkonto und vieles mehr).¹

Mit anderen Worten: Eine Identität ist eine in ihrem Verwendungskontext eindeutige, wiedererkennbare Beschreibung einer natürlichen oder juristischen Person oder eines Objektes z. B. Personengruppe, Unternehmen, Rechner, Programm, Datei, die sich aus Attributen, also den Eigenschaften einer Identität, und einem Identitätsbezeichner zusammensetzt, womit ein beliebiger Name gemeint ist, der die Attribute auf sich vereint und der echt, gefälscht oder von Dritten (einvernehmlich) gegeben worden sein kann. Einfacher ausgedrückt: Die Identität einer Person bildet die Grundlage für ihre Rechtspersönlichkeit. Im tatsächlichen Leben definiert sich diese Identität durch den Personenstand, diese wird zudem durch das Gesetz geschützt. In der virtuellen Welt reicht die Identität einer Person viel weiter und ist weniger klar umrissen. Einige digitale Daten, die die Identität einer Person betreffen (z. B. Kontodaten, Benutzernamen und Kennwörter) ermöglichen den Zugang zu privaten Daten. All diese digitalen Identifizierungsmerkmale, die nicht als Elemente der Rechtspersönlichkeit einer Person betrachtet werden, werden immer begehrter.

Der Begriff Identitätsdiebstahl beschreibt zunächst nur die ungestattete, rechtswidrige Beschaffung fremder, bestehender Identitätsmerkmale im Sinne von Identitätsbezeichnern.

Zum Beispiel: Internationale Betrügerbanden schalten gefälschte Stellenanzeigen in Internet-Jobbörsen oder versenden diese per E-Mail. Sie spähen Bewerber aus, stehlen deren Identität oder betrügen sie um viel Geld - überwiesen für angebliche Vermittlungsgebühren oder Spezialsoftware. Daneben werden im Zusammenhang mit dem Cybercrime häufig Identitätstauschungen durchgeführt, bei denen zunächst eine meist nur rudimentäre Identität generiert (entwickelt oder gestohlen; Phishing, Skimming, Carding) und dann zu eigenen Zwecken missbraucht wird. Bei der Betrachtung der Handlungen muss zwischen der Edition (Beschaffung, Gestaltung) von persönlichkeitsbestimmenden Merkmalen und ihrer

¹ Georg Borges, Jörg Schwenk, Carl-Friedrich Stuckenberg, Christoph Wegener, in: Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte.

Verwendung im kriminellen Zusammenhang unterschieden werden. Allgemein ist das Vorkommen von diesen Phänomenen überwiegend negativ konnotiert und erfolgt mit Schädigungsabsicht.²

Die Schufa hat für geschädigte Personen eigens eine Liste mit Identitätsbetrugsoffern erstellt, welche einem Bericht der WELT AM SONNTAG vom 17.07.2022 inzwischen über 7.000 Verbraucherinnen und Verbraucher in Deutschland umfasst. Geschädigte Personen berichten allerdings, dass diese sich von Polizei und Staatsanwaltschaft häufig allein gelassen fühlen. Da die Täterinnen und Täter ihre IP-Adresse mittels VPN-Server legal verschleiern, würden Ermittlungsverfahren häufig eingestellt.

Die Folgen für betroffene Personen sind teilweise gravierend.

Betrügerinnen und Betrüger können im Internet im Namen der geschädigten Personen Waren und Dienstleistungen bestellen. Geschädigte Personen erhalten davon meist erst dann Kenntnis, wenn diese Rechnungen für Waren und Dienstleistungen erhalten, welche diese nie bestellt haben. Werden die Rechnungen nicht bezahlt, folgt ein Negativeintrag bei der Schufa. Hierbei kommt es nicht selten vor, dass die Schädigung der Kreditwürdigkeit erst später aufgedeckt wird, wenn plötzlich die Finanzierung eines Autos oder einer Hypothek ins Haus steht und die Kreditvergabe verweigert wird.

Das Interesse der Täterinnen und Täter geht meist über finanzielle Informationen wie Bankkontonummern hinaus. Sie zeigen überaus großes Interesse an persönlichen Daten wie zum Beispiel Geburtsdatum, Adresse und Personalausweisnummer. Sind die Kriminellen einmal im Besitz dieser sensiblen Daten, können sie einen Führerschein beantragen, Leistungen beziehen oder Anstellungen erschleichen. Opfer müssen sich auch ggf. mit der Strafverfolgung auseinandersetzen, wenn die Identität ohne Wissen der Opfer für die Begehung von Straftaten genutzt wurde.

In der Regel wird ein Identitätsdiebstahl erst spät bemerkt und oft sind dann bereits beträchtliche Schäden entstanden, zum Beispiel Betrugsanklagen, Mahnverfahren oder Negativeinträge in der Schufa. Für die Opfer ist es vielfach schwer, ihre „Unschuld“ nachzuweisen und die zeitliche, finanzielle und psychische Belastungen sind enorm.

Auch der öffentlichen Hand können Schäden entstehen. So kann es durch Identitätsdiebstahl zu Subventionsbetrug kommen oder auch zum Steuerbetrug. Steuerlicher Identitätsdiebstahl liegt vor, wenn jemand die Sozialversicherungsnummer einer anderen Person verwendet, um eine falsche Steuererklärung einzureichen und eine Rückerstattung zu beantragen. Identitätsdiebe können auch staatliche Leistungen wie Arbeitslosengeld erhalten.

Vor diesem Hintergrund fragen wir die Landesregierung:

1. Wie haben sich die Fälle von Identitätsdiebstahl in den letzten fünf Jahren entwickelt?
2. Wie hoch ist die Aufklärungsquote der in diesem Zeitraum bekanntgewordenen Fälle? (Bitte übersichtsartig darstellen, wie viele Strafanzeigen es gab, wie viele Ermittlungsverfahren durchgeführt wurden und wie viele Verfahren aus welchen Gründen eingestellt wurden.)

² Kochheim, Cybercrime, Rn. 480 ff.

3. Welcher wirtschaftlicher Schaden entsteht durch dieses Kriminalitätsphänomen?
4. Welcher Schaden (bspw. in Form von Subventionsbetrug, Erschleichung von Leistungen, Corona – Hilfen, Steuerbetrug) ist dem Land Nordrhein-Westfalen in den letzten zwei Jahren durch dieses Kriminalitätsphänomen entstanden?
5. Welche Maßnahmen plant die Landesregierung, um Identitätsdiebstahl stärker zu bekämpfen, die Aufklärung zu verbessern und Opfer besser zu unterstützen?

Angela Freimuth
Marc Lübke

29.09.2022

Antwort

der Landesregierung

auf die Kleine Anfrage 358 vom 23. August 2022
der Abgeordneten Angela Freimuth und Marc Lürbke FDP
Drucksache 18/659

Was unternimmt die Landesregierung gegen Identitätsdiebstahl?

Vorbemerkung der Kleinen Anfrage

Die Identität ist eine den Bewertungszusammenhang betreffende, insoweit flexible Summe aus persönlichen Merkmalen, die eine interaktive Person ausmachen. Dabei kann es sich um eine fragmentierte Person handeln, die nur durch wenige Eigenschaften bestimmt ist (Kontoinhaber, Nickname und Avatar in einer Spiel- oder Kommunikationsumgebung), bis hin zu einem existierenden Menschen in einer vollständigen gesellschaftlichen Umgebung mit ihren diversen Schnittstellen (Melderegister, Sozialversicherungsnummer, Bankkonto und vieles mehr).¹

Mit anderen Worten: Eine Identität ist eine in ihrem Verwendungskontext eindeutige, wiedererkennbare Beschreibung einer natürlichen oder juristischen Person oder eines Objektes z. B. Personengruppe, Unternehmen, Rechner, Programm, Datei, die sich aus Attributen, also den Eigenschaften einer Identität, und einem Identitätsbezeichner zusammensetzt, womit ein beliebiger Name gemeint ist, der die Attribute auf sich vereint und der echt, gefälscht oder von Dritten (einvernehmlich) gegeben worden sein kann. Einfacher ausgedrückt: Die Identität einer Person bildet die Grundlage für ihre Rechtspersönlichkeit. Im tatsächlichen Leben definiert sich diese Identität durch den Personenstand, diese wird zudem durch das Gesetz geschützt. In der virtuellen Welt reicht die Identität einer Person viel weiter und ist weniger klar umrissen. Einige digitale Daten, die die Identität einer Person betreffen (z. B. Kontodaten, Benutzernamen und Kennwörter) ermöglichen den Zugang zu privaten Daten. All diese digitalen Identifizierungsmerkmale, die nicht als Elemente der Rechtspersönlichkeit einer Person betrachtet werden, werden immer begehrt.

Der Begriff Identitätsdiebstahl beschreibt zunächst nur die ungestattete, rechtswidrige Beschaffung fremder, bestehender Identitätsmerkmale im Sinne von Identitätsbezeichnern.

Zum Beispiel: Internationale Betrügerbanden schalten gefälschte Stellenanzeigen in Internet-Jobbörsen oder versenden diese per E-Mail. Sie spähen Bewerber aus, stehlen deren Identität oder betrügen sie um viel Geld - überwiesen für angebliche Vermittlungsgebühren oder Spezialsoftware. Daneben werden im Zusammenhang mit dem Cybercrime häufig

¹ Georg Borges, Jörg Schwenk, Carl-Friedrich Stuckenberg, Christoph Wegener, in: Identitätsdiebstahl und Identitätsmissbrauch im Internet. Rechtliche und technische Aspekte.

Identitätstauschungen durchgeführt, bei denen zunächst eine meist nur rudimentäre Identität generiert (entwickelt oder gestohlen; Phishing, Skimming, Carding) und dann zu eigenen Zwecken missbraucht wird. Bei der Betrachtung der Handlungen muss zwischen der Edition (Beschaffung, Gestaltung) von persönlichkeitsbestimmenden Merkmalen und ihrer Verwendung im kriminellen Zusammenhang unterschieden werden. Allgemein ist das Vorkommen von diesen Phänomenen überwiegend negativ konnotiert und erfolgt mit Schädigungsabsicht.²

Die Schufa hat für geschädigte Personen eigens eine Liste mit Identitätsbetrugsoffern erstellt, welche einem Bericht der WELT AM SONNTAG vom 17.07.2022 inzwischen über 7.000 Verbraucherinnen und Verbraucher in Deutschland umfasst. Geschädigte Personen berichten allerdings, dass diese sich von Polizei und Staatsanwaltschaft häufig allein gelassen fühlen. Da die Täterinnen und Täter ihre IP-Adresse mittels VPN-Server legal verschleiern, würden Ermittlungsverfahren häufig eingestellt.

Die Folgen für betroffene Personen sind teilweise gravierend.

Betrügerinnen und Betrüger können im Internet im Namen der geschädigten Personen Waren und Dienstleistungen bestellen. Geschädigte Personen erhalten davon meist erst dann Kenntnis, wenn diese Rechnungen für Waren und Dienstleistungen erhalten, welche diese nie bestellt haben. Werden die Rechnungen nicht bezahlt, folgt ein Negativeintrag bei der Schufa. Hierbei kommt es nicht selten vor, dass die Schädigung der Kreditwürdigkeit erst später aufgedeckt wird, wenn plötzlich die Finanzierung eines Autos oder einer Hypothek ins Haus steht und die Kreditvergabe verweigert wird.

Das Interesse der Täterinnen und Täter geht meist über finanzielle Informationen wie Bankkontonummern hinaus. Sie zeigen überaus großes Interesse an persönlichen Daten wie zum Beispiel Geburtsdatum, Adresse und Personalausweisnummer. Sind die Kriminellen einmal im Besitz dieser sensiblen Daten, können sie einen Führerschein beantragen, Leistungen beziehen oder Anstellungen erschleichen. Opfer müssen sich auch ggf. mit der Strafverfolgung auseinandersetzen, wenn die Identität ohne Wissen der Opfer für die Begehung von Straftaten genutzt wurde.

In der Regel wird ein Identitätsdiebstahl erst spät bemerkt und oft sind dann bereits beträchtliche Schäden entstanden, zum Beispiel Betrugsanklagen, Mahnverfahren oder Negativeinträge in der Schufa. Für die Opfer ist es vielfach schwer, ihre „Unschuld“ nachzuweisen und die zeitliche, finanzielle und psychische Belastungen sind enorm.

Auch der öffentlichen Hand können Schäden entstehen. So kann es durch Identitätsdiebstahl zu Subventionsbetrug kommen oder auch zum Steuerbetrug. Steuerlicher Identitätsdiebstahl liegt vor, wenn jemand die Sozialversicherungsnummer einer anderen Person verwendet, um eine falsche Steuererklärung einzureichen und eine Rückerstattung zu beantragen. Identitätsdiebe können auch staatliche Leistungen wie Arbeitslosengeld erhalten.

Der Minister der Justiz hat die Kleine Anfrage 358 mit Schreiben vom 29. September 2022 namens der Landesregierung im Einvernehmen mit dem Minister des Innern und der Ministerin für Landwirtschaft und Verbraucherschutz beantwortet.

² Kochheim, Cybercrime, Rn. 480 ff.

1. **Wie haben sich die Fälle von Identitätsdiebstahl in den letzten fünf Jahren entwickelt?**
2. **Wie hoch ist die Aufklärungsquote der in diesem Zeitraum bekanntgewordenen Fälle? (Bitte übersichtsartig darstellen, wie viele Strafanzeigen es gab, wie viele Ermittlungsverfahren durchgeführt wurden und wie viele Verfahren aus welchen Gründen eingestellt wurden.)**
3. **Welcher wirtschaftliche Schaden entsteht durch dieses Kriminalitätsphänomen?**

Die Fragen 1 bis 3 werden gemeinsam beantwortet.

Dem Ministerium des Innern dient als Datenbasis für die Beantwortung der Fragen 1 bis 3 die Polizeiliche Kriminalstatistik Nordrhein-Westfalen. Diese bildet seit dem 01.01.2019 Fallzahlen für das Phänomen „Digitaler Identitätsdiebstahl“ ab.

Die Erfassung von Fällen, Tatverdächtigen und Opfern in der Polizeilichen Kriminalstatistik erfolgt nach bundeseinheitlichen Richtlinien.

Die Anzahl der bekannt gewordenen Fälle des Phänomens „Digitaler Identitätsdiebstahl“ bitte ich der Anlage 1 zu entnehmen. Gesondert erfasste Auslandstaten sind diejenigen Fälle, in denen die/der Tatverdächtige im Ausland handelt und der Erfolg in Deutschland eintritt oder eintreten soll. Die Anlage 2 enthält Informationen über entstandene finanzielle Schäden. Die dort enthaltenen Daten sind unter der Maßgabe zu betrachten, dass zu den Delikten „Ausspähen, Abfangen von Daten, einschließlich Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB“ in der Polizeilichen Kriminalstatistik kein finanzieller Schaden erfasst wird und dieser demnach auch nicht mit in die Summen der Anlage 2 eingeflossen ist.

Statistische Zahlen zu Verurteilungen oder Einstellungen von Verfahren liegen dem Ministerium des Innern nicht vor.

Auch justizielle statistische Erhebungen im Sinne der Anfrage liegen nicht vor. Dementsprechend bedürfte es zur validen Beantwortung der Fragen 1 bis 3, soweit der Geschäftsbereich des Ministeriums der Justiz berührt ist, einer händischen Auswertung sämtlicher in Betracht kommender Verfahren, die mit vertretbarem Verwaltungsaufwand nicht zu leisten ist.

4. **Welcher Schaden (bspw. in Form von Subventionsbetrug, Erschleichung von Leistungen, Corona – Hilfen, Steuerbetrug) ist dem Land Nordrhein-Westfalen in den letzten zwei Jahren durch dieses Kriminalitätsphänomen entstanden?**

Eine Aussage zu dem Schaden, der dem Land Nordrhein-Westfalen entstanden ist, kann auf Basis der Polizeilichen Kriminalstatistik nicht getroffen werden, da die Polizeiliche Kriminalstatistik als Opfer lediglich natürliche Personen erfasst. Auch im Geschäftsbereich des Ministeriums der Justiz liegen hierzu keine statistischen Erhebungen vor.

Eine manuelle Überprüfung der Verfahren zur Feststellung des dem Land Nordrhein-Westfalen entstandenen Schadens ist mit vertretbarem Verwaltungsaufwand nicht zu leisten.

5. Welche Maßnahmen plant die Landesregierung, um Identitätsdiebstahl stärker zu bekämpfen, die Aufklärung zu verbessern und Opfer besser zu unterstützen?

Für die Landesregierung ist die Kriminalprävention ein bedeutender Schwerpunkt ihres Handelns. Kriminalprävention ist dabei eine gesamtgesellschaftliche Aufgabe, die vernetzt, interdisziplinär und als ressort- und institutionsübergreifende Kooperation auf mehreren Ebenen umgesetzt werden muss.

Landeskampagne der Polizei NRW „Mach Dein Passwort stark“

Die landesweite Präventionskampagne „Mach dein Passwort stark“ (www.mach-dein-passwort-stark.de) stellt zielgruppengerecht Informationen zur Verfügung. Beinhaltet sind Filme und Podcasts sowie weiterführende Hinweise zu den Kooperationspartnern: Verbraucherzentrale Nordrhein-Westfalen, Bundesamt für Sicherheit in der Informationstechnik und dem eco-Verband der Internetwirtschaft e. V.

Die durchgeführte wissenschaftliche Evaluation dieser Kampagne konnte resultierenden Wissenszuwachs und Verhaltensänderungen bei der Zielgruppe belegen.

Öffentlichkeitsarbeit

Die Netzredaktion des Landeskriminalamts Nordrhein-Westfalen hat in diesem Jahr bereits Social-Media-Beiträge zu den folgenden Themen veröffentlicht:

- Betrug Online-Kleinanzeigen
- Erpresserische E-Mails i. Z. m. Ukraine
- Daten sichern und schützen
- Warnung Anruf „Europol/Interpol“
- Digitaler „Frühjahrsputz“ Digitale Türen und Fenster absichern
- Warnung Phishing i. Z. Ukraine
- Identitätsdiebstahl/Online-Vortrag Mach dein Passwort stark
- Mach dein Passwort stark/Kampagne B. Steinhaus
- Schutz vor Betrug im Netz

Alle Beiträge behandelten auch die Thematik „Identitätsdiebstahl“. Durch das Teilen der Beiträge wurde eine sechsstellige Anzahl von Bürgerinnen und Bürgern erreicht.

Darüber hinaus enthält die Website polizei.nrw/cybercrime umfangreiche Informationen, unter anderem auch zu der hier in Rede stehenden Thematik.

Maßnahmen der Kreispolizeibehörden

Die für Kriminalprävention zuständigen Kriminalkommissariate der Kreispolizeibehörden stellen in ihren jeweiligen lokalen Netzwerken in Einzel- und Gruppenberatungen Informationsmaterial zum Schutz vor Identitätsdiebstahl Verfügung.

Koordinierungsstelle Cybersicherheit

Die nordrhein-westfälische Landesregierung hat bereits im Jahr 2020 die Einrichtung einer Koordinierungsstelle für Cybersicherheit im Rahmen der Cybersicherheitsstrategie Nordrhein-Westfalen beschlossen. Die dort entwickelten Strategien und Herangehensweisen behandeln auch das hier in Rede stehende Phänomen. Die Koordinierungsstelle Cybersicherheit Nordrhein-Westfalen stellt diverse Informationsangebote zur Verfügung, um ein Bewusstsein für die damit verbundenen Gefahren zu schaffen. Dazu gehören zum Beispiel die Website cybersicherheit.nrw und der jährlich erscheinende Bericht zur Cybersicherheit in Nordrhein-

Westfalen. Sowohl der Webauftritt als auch der Cybersicherheitsbericht werden laufend aktualisiert und weiterentwickelt.

Überdies hält die von der Landesregierung institutionell geförderte Verbraucherzentrale NRW ein umfangreiches Angebot vor, um Verbraucherinnen und Verbraucher auch in Zukunft für das Thema Datenschutz und IT-Sicherheit zu sensibilisieren, über Risiken aufzuklären und ihnen Instrumente zur „digitalen Selbstverteidigung“ an die Hand zu geben.

Im Rahmen von Bildungsangeboten der Verbraucherzentrale NRW werden Vorträge in Schulen, bei Initiativen und zahlreichen Kooperationspartnern in verschiedenen NRW-Städten gehalten. Dies geschieht in Form von Vortragsveranstaltungen vor Ort sowie digital zu Themen wie „Passwortsicherheit“ oder „Maßnahmen zur Erhöhung der Sicherheit im Internet“. Darüber hinaus wurde zum Safer Internet Day 2022 der digitale Selbstlernkurs „Meine Daten – alles OK im www“ erfolgreich eingeführt (<https://www.verbraucherzentrale.nrw/meine-daten>). Weitere Lerneinheiten sind geplant.

Die bestehende enge Kooperation der Verbraucherzentrale NRW mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Landeskriminalamt (LKA) wird fortgesetzt. Im Fokus steht dabei vor allem die inhaltliche Zusammenarbeit z.B. in Form von Aktionen, Kampagnen und Workshops sowie die gemeinsame Erstellung von Material (wie der Flyer „Schadprogramme – So schützen Sie sich.“ oder „Die SOS-Karte – Schutz beim Onlineshopping“). Im Rahmen des „Phishing-Radars“ veröffentlicht die Verbraucherzentrale NRW in ihrem Internetangebot Informationen und Meldungen rund um gefakte E-Mails oder Internetseiten, um vor aktuellen Angriffen in Bezug auf Identitätsdiebstahl und das Ausspähen von sicherheitsrelevanten persönlichen Daten zu warnen. Die Meldungen des „Phishing-Radars“ werden monatlich auch dem BSI zur Verfügung gestellt.

Auf der Website der Verbraucherzentrale werden zahlreiche Online-Artikel zu Themen im Bereich Datenschutz und Datensicherheit in der digitalen Welt, (z. B. Malware/Ransomware, Identitätsdiebstahl, Cybercrime), veröffentlicht. Mit digitalen Anwendungen, wie dem Fake-shop-Finder, können Verbraucherinnen und Verbraucher unseriöse Online-Shops im Internet erkennen.

Schließlich gehen die dem Legalitätsprinzip verpflichteten Staatsanwaltschaften des Landes Nordrhein-Westfalen konsequent gegen sämtliche ihnen bekannt werdenden strafbaren Formen des Identitätsdiebstahls vor. Bei ihrer Arbeit legen sie stets auch ein besonderes Augenmerk auf die Belange des Opferschutzes, denn die Folgen eines Identitätsdiebstahls können für die Opfer gravierend sein und diese über einen langen Zeitraum begleiten. Betroffene von Identitätsdiebstahl können sich jederzeit vertrauensvoll an die Strafverfolgungsbehörden wenden, auch wenn sie sich selbst mit vermeintlich strafrechtlichen Vorwürfen konfrontiert sehen. Auch die Opferschutzbeauftragte des Landes Nordrhein-Westfalen kann ihnen aufgrund ihrer praktischen Erfahrungen beratend zur Seite stehen.

Phänomen 'Digitaler Identitätsdiebstahl' für die Berichtsjahre 2019 bis 2021

Anzahl bekannt gewordener Fälle - Anzahl aufgeklärter Fälle - AQ in %

Berichtsjahr	Schl.-Zahl	Straftat	Fälle						
			bekannt geworden	davon:					
				Inlandsstraftaten			Auslandsstraftaten		
				bekannt geworden	<u>davon</u> aufgeklärt	AQ in %	bekannt geworden	<u>davon</u> aufgeklärt	AQ in %
1	2	3	4	5	6	7	8	9	10
2021	Straftaten insgesamt	3 480	1 508	415	27,52	1 972	47	2,38
2020	Straftaten insgesamt	2 671	1 390	425	30,58	1 281	26	2,03
2019	Straftaten insgesamt	2 103	1 121	230	20,52	982	19	1,93

Quelle: PKS NRW

Phänomen 'Digitaler Identitätsdiebstahl' für die Berichtsjahre 2019 bis 2021
Schadenssumme in Euro

Berichtsjahr	Schl.-Zahl	Straftat	Schadenssumme in Euro		
			insgesamt	davon:	
				Inlandsstraftaten	Auslandsstraftaten
1	2	3	4	5	6
2021	Straftaten insgesamt	2 288 595	543 620	1 744 975
2020	Straftaten insgesamt	1 479 502	520 549	958 953
2019	Straftaten insgesamt	1 237 667	727 933	509 734

Quelle: PKS NRW