

Inhaltsübersicht

| | |
|---|----|
| Inhaltsverzeichnis | 11 |
| Abkürzungsverzeichnis | 21 |
| Kapitel 1: Einführung | 25 |
| A. Einleitung | 25 |
| B. Künstliche Intelligenz | 27 |
| I. Big Data | 28 |
| II. Künstliche Intelligenz | 29 |
| III. KI-Anwendungen | 34 |
| IV. KI versus Big Data | 36 |
| C. Künstliche Intelligenz unter dem Begriff der Rechtswissenschaft | 37 |
| I. Europäische Perspektive | 38 |
| II. Taiwans Perspektive | 45 |
| III. Zwischenfazit | 46 |
| D. Die Bedeutung des Einsatzes von künstlicher Intelligenz in der Strafverfolgung | 48 |
| I. Schwierige Abgrenzung zwischen Strafverfolgung und polizeiliche Gefahrenabwehr | 49 |
| II. Künstliche Intelligenz als Hilfsmittel der Strafverfolgung | 53 |
| Kapitel 2: Der Einsatz von KI in der Strafverfolgung zur Verbrechensbekämpfung | 55 |
| A. Der aktuelle Einsatz in der Strafverfolgung | 55 |
| I. Ein erkennbares System zur Strafverfolgung | 56 |
| II. Prognosesysteme zur Strafverfolgung | 76 |
| III. Chinas AI Staatsanwalt – Der automatisierte Ankläger | 84 |
| IV. Zwischenfazit | 86 |
| B. Der Vorteil für KI als Ermittlungsmaßnahme | 87 |
| I. Kriminalität durch künstliche Intelligenz | 87 |
| II. Verbrechensbekämpfung | 89 |

| | |
|---|--------|
| III. Effektiver und schneller durch KI | 90 |
| C. Problem des aktuellen Einsatzes bei Strafverfolgungen | 91 |
| I. Grundrechtsverletzung | 91 |
| II. Intransparenz | 93 |
| III. Diskriminierungsprobleme | 94 |
| IV. Genauigkeitsprobleme | 95 |
| V. Automation Complacency | 96 |
| Kapitel 3: Rechtliche Auswirkungen des Einsatzes von KI in der Strafverfolgung | 99 |
| A. Auswirkung der Nutzung von personenbezogenen Daten | 99 |
| I. Das Recht auf informationelle Selbstbestimmung in Deutschland | 99 |
| II. Spannungsfeld im deutschen Datenschutzrecht | 102 |
| III. Die Bedeutung der persönlichen Informationsselbstbestimmung im taiwanesischen Recht | 114 |
| IV. Taiwanesisches Gesetz zum Schutz persönlicher Daten | 116 |
| V. Zwischenfazit | 120 |
| B. Probleme der Rechtsquelle | 121 |
| I. Deutsches Strafprozessrecht | 122 |
| II. Taiwanesisches Strafprozessrecht | 127 |
| III. Zwischenfazit | 130 |
| C. Systematische Fehlerproblematik | 131 |
| I. Die Objektivität des algorithmischen Systems | 131 |
| II. Begriff der Diskriminierung | 132 |
| III. Systematische Diskriminierung | 133 |
| IV. Ermittlungen von diskriminierenden Fragen durch künstliche Intelligenz | 135 |
| D. Künstliche Intelligenz und die Unschuldsvermutung | 141 |
| I. Grundsatz der Unschuldsvermutung | 141 |
| II. Strafverfolgung durch KI und Widerspruch zum Prinzip der Unschuldsvermutung | 146 |

| | |
|--|-----|
| Kapitel 4: Gegenmaßnahmen zu den Problemen | 149 |
| A. Meinung auf EU-Ebene | 149 |
| I. Ethische Charta für CEPEJ | 149 |
| II. KI-Verordnung | 154 |
| B. Die Verfassungswidrigkeit von hessenDATA | 164 |
| I. Sachverhalt | 164 |
| II. Beurteilung durch das Bundesverfassungsgericht (BVerfG) | 165 |
| III. Neues HSOG | 174 |
| IV. Zwischenfazit | 181 |
| C. England – Edward Bridges Urteil | 183 |
| I. Sachverhalt | 183 |
| II. The Divisional Court’s judgment | 184 |
| III. Ansichten von HIGH COURT | 188 |
| IV. Zwischenfazit | 193 |
| D. Niederländisches Fall-System SyRI | 197 |
| I. Sachverhalt | 197 |
| II. Die Feststellung des Gerichts | 198 |
| III. Zwischenfazit | 203 |
| E. Japans Blick | 205 |
| I. N-System-Urteil | 205 |
| II. Japanische Ansicht zum Gesichtserkennungssystem | 209 |
| III. Zwischenfazit | 220 |
| F. Taiwans Blick | 223 |
| I. Untersuchung von Kryptowährungen oder virtuellen Währungen | 225 |
| II. Überdenken des Einsatzes von künstlicher Intelligenz bei der Strafverfolgung durch technologische Ermittlungsanwendungen | 232 |
| G. Zwischenfazit | 243 |
| Kapitel 5: Zusammenfassung der Schlussfolgerungen | 247 |
| A. Zusammenfassung | 247 |
| B. Vorschläge | 248 |
| I. Eine gewisse objektive Tatsache als Voraussetzung | 248 |

Inhaltsübersicht

| | |
|---|-----|
| II. Spezifische Verbrechen | 250 |
| III. Notwendigkeit des Richtervorbehalts | 251 |
| IV. Verhältnismäßigkeit | 253 |
| V. Menschliche Autonomie und Kontrolle | 255 |
| VI. Risikobewertung und Datenschutzmanagement | 256 |
| VII. Gewährleistung von Transparenz | 258 |
| VIII. Rechtsbehelfe | 259 |
| IX. Erfassung und Verfolgung von Verantwortlichkeiten | 260 |
| X. Strenge Regeln für den Ausschluss unzulässiger Beweismittel | 260 |
| Literaturverzeichnis | 263 |

Inhaltsverzeichnis

| | |
|--|----|
| Abkürzungsverzeichnis | 21 |
| Kapitel 1: Einführung | 25 |
| A. Einleitung | 25 |
| B. Künstliche Intelligenz | 27 |
| I. Big Data | 28 |
| II. Künstliche Intelligenz | 29 |
| 1. Die Bedeutung der „künstlichen Intelligenz“ | 29 |
| 2. Schwache und starke künstliche Intelligenz | 31 |
| 3. Die Algorithmen | 32 |
| III. KI-Anwendungen | 34 |
| IV. KI versus Big Data | 36 |
| C. Künstliche Intelligenz unter dem Begriff der Rechtswissenschaft | 37 |
| I. Europäische Perspektive | 38 |
| 1. Entwurf eines EU-Gesetzes über künstliche Intelligenz im Jahr 2021 und 2022 | 38 |
| 2. Entwurf eines EU-Gesetzes über künstliche Intelligenz im Jahr 2023 | 41 |
| 3. Finale Fassung der Verordnung über künstliche Intelligenz (2024) | 43 |
| II. Taiwans Perspektive | 45 |
| III. Zwischenfazit | 46 |
| D. Die Bedeutung des Einsatzes von künstlicher Intelligenz in der Strafverfolgung | 48 |
| I. Schwierige Abgrenzung zwischen Strafverfolgung und polizeiliche Gefahrenabwehr | 49 |
| 1. Festlegung der Grenzen auf Ebene der Regulierung | 50 |
| 2. KI-VO | 52 |
| 3. Zwischenfazit | 52 |
| II. Künstliche Intelligenz als Hilfsmittel der Strafverfolgung | 53 |

| | |
|--|----|
| Kapitel 2: Der Einsatz von KI in der Strafverfolgung zur Verbrechensbekämpfung | 55 |
| A. Der aktuelle Einsatz in der Strafverfolgung | 55 |
| I. Ein erkennbares System zur Strafverfolgung | 56 |
| 1. Objekt- und Bilderkennungssystem | 56 |
| a) Kennzeichenerkennung in Deutschland | 56 |
| b) Kennzeichenerkennung in Taiwan und Japan | 58 |
| aa) Taiwans Kennzeichenerkennung | 58 |
| bb) Japans N-System | 61 |
| 2. Gesichtserkennung | 62 |
| a) England – Edward Bridges | 63 |
| b) USA – Clearview | 64 |
| c) Taiwans M-Police | 66 |
| d) Chinas Sky Net und Social Credit System | 68 |
| 3. Videoanalysen im Bereich des sexuellen Kindesmissbrauchs | 69 |
| 4. Ort der Schussgeräusche | 71 |
| 5. Medienaufsicht gegen Verbrechen in Deutschland | 73 |
| 6. Zwischenfazit | 75 |
| II. Prognosesysteme zur Strafverfolgung | 76 |
| 1. Raumbezogene Verfahren | 77 |
| a) Hot-Spot-Methoden | 77 |
| b) Near Repeat-Prognostik | 78 |
| c) Risk Terrain Analysis | 80 |
| 2. Personenbezogene Verfahren | 81 |
| a) USA-strategische Subjektliste der Chicagoer Polizei | 82 |
| b) Deutschland – Gotham System | 83 |
| c) Taiwans Drogendatenbank | 84 |
| III. Chinas AI Staatsanwalt – Der automatisierte Ankläger | 84 |
| IV. Zwischenfazit | 86 |
| B. Der Vorteil für KI als Ermittlungsmaßnahme | 87 |
| I. Kriminalität durch künstliche Intelligenz | 87 |
| II. Verbrechensbekämpfung | 89 |
| III. Effektiver und schneller durch KI | 90 |
| C. Problem des aktuellen Einsatzes bei Strafverfolgungen | 91 |
| I. Grundrechtsverletzung | 91 |
| II. Intransparenz | 93 |

| | |
|---|--------|
| III. Diskriminierungsprobleme | 94 |
| IV. Genauigkeitsprobleme | 95 |
| V. Automation Complacency | 96 |
| Kapitel 3: Rechtliche Auswirkungen des Einsatzes von KI in der Strafverfolgung | 99 |
| A. Auswirkung der Nutzung von personenbezogenen Daten | 99 |
| I. Das Recht auf informationelle Selbstbestimmung in Deutschland | 99 |
| II. Spannungsfeld im deutschen Datenschutzrecht | 102 |
| 1. Keine gesetzliche Regelung und Schwierigkeiten bei der Anonymisierung | 103 |
| 2. Verstoß gegen das Gebot der Angemessenheit und Transparenz | 104 |
| 3. Probleme mit der Zweckbindung | 107 |
| 4. Verstoß gegen das Verbot des Automatisierungsbeschlusses | 108 |
| 5. Gegen den Grundsatz der Datenminimierung | 111 |
| 6. Herausforderungen der Datenlöschung | 112 |
| III. Die Bedeutung der persönlichen Informationsselbstbestimmung im taiwanesischen Recht | 114 |
| IV. Taiwanesisches Gesetz zum Schutz persönlicher Daten | 116 |
| 1. Ordnungsgemäßer Zweck der Datenerhebung und -verwendung | 117 |
| 2. Ausnahmen von der Datenerhebung und -verwendung | 118 |
| a) Gesetz als Ausnahme | 118 |
| b) Der Schutz eines erheblichen öffentlichen Interesses | 119 |
| c) Deidentifizierung von Daten | 120 |
| V. Zwischenfazit | 120 |
| B. Probleme der Rechtsquelle | 121 |
| I. Deutsches Strafprozessrecht | 122 |
| 1. Rasterfahndung | 122 |
| 2. Technische Ermittlungen in der StPO als Rechtsquelle? | 124 |
| 3. Allgemeine Ermittlungsbefugnis | 127 |
| II. Taiwanesisches Strafprozessrecht | 127 |
| III. Zwischenfazit | 130 |

| | |
|---|-----|
| C. Systematische Fehlerproblematik | 131 |
| I. Die Objektivität des algorithmischen Systems | 131 |
| II. Begriff der Diskriminierung | 132 |
| III. Systematische Diskriminierung | 133 |
| 1. Induktive Bias | 133 |
| 2. Statistische Bias | 134 |
| 3. Kognitive Verzerrungen | 134 |
| IV. Ermittlungen von diskriminierenden Fragen durch künstliche Intelligenz | 135 |
| 1. Verzerrung bei der Ermessensentscheidung | 135 |
| 2. Übermäßige Fehlerabhängigkeit | 136 |
| 3. Auswirkungen der Intransparenz der Blackbox | 139 |
| a) Grundsätze für ein ordnungsgemäßes Rechtsverfahren | 139 |
| b) Argumente gegen ein ordnungsgemäßes Rechtsverfahren beim Einsatz von KI | 140 |
| D. Künstliche Intelligenz und die Unschuldsvermutung | 141 |
| I. Grundsatz der Unschuldsvermutung | 141 |
| 1. Geschichte | 141 |
| 2. Unschuldsvermutung und Strafverfolgung | 144 |
| II. Strafverfolgung durch KI und Widerspruch zum Prinzip der Unschuldsvermutung | 146 |
| 1. Argumente gegen die Verhältnismäßigkeit | 146 |
| 2. Die Frage des Anfangsverdachts | 147 |
| Kapitel 4: Gegenmaßnahmen zu den Problemen | 149 |
| A. Meinung auf EU-Ebene | 149 |
| I. Ethische Charta für CEPEJ | 149 |
| 1. Grundsatz der Achtung der Menschenrechte | 150 |
| 2. Grundsatz der Nichtdiskriminierung | 151 |
| 3. Grundsatz der Qualität und Sicherheit | 151 |
| 4. Grundsatz der Transparenz, Unabhängigkeit und Fairness | 152 |
| 5. Grundsatz der Gewährleistung menschlicher Intervention | 153 |

| | |
|--|-----|
| II. KI-Verordnung | 154 |
| 1. Gesichtserkennungssystem für Zwecke der Strafverfolgung | 155 |
| a) Gesetzesentwurf über künstliche Intelligenz im Jahr 2021 | 155 |
| aa) Öffentliche Interessen | 155 |
| bb) Der Grundsatz der vorherigen Genehmigung | 156 |
| cc) Angemessene Schutzmaßnahmen und Voraussetzungen | 156 |
| b) Gesetzesentwurf über künstliche Intelligenz im Jahr 2023 | 157 |
| c) Neue KI-VO in Jahr 2024 | 159 |
| aa) Genehmigungspflicht | 159 |
| bb) Verhältnismäßigkeit der Verwendung | 160 |
| cc) Melde- und Mitteilungspflichten | 161 |
| 2. Andere Anwendungen künstlicher Intelligenz in der Strafverfolgung | 161 |
| B. Die Verfassungswidrigkeit von hessenDATA | 164 |
| I. Sachverhalt | 164 |
| II. Beurteilung durch das Bundesverfassungsgericht (BVerfG) | 165 |
| 1. Die Grundsätze der Zweckbindung und Zweckänderung für Datenerhebungseingriffe | 165 |
| a) Zweckwahrende Weiterverwendung | 166 |
| b) Zweckänderungen | 166 |
| c) Daten der Wohnraumüberwachung und Online-Durchsuchung | 167 |
| d) Zwischenfazit | 167 |
| 2. Belastungswirkung durch automatisierte Analyse | 167 |
| 3. Eingriffsintensität | 168 |
| 4. Verfassungsrechtliche Anforderungen an die automatisierte Analyse | 170 |
| a) Rechtfertigung unter engen Voraussetzungen | 170 |
| b) Verringerung des Eingriffs | 171 |
| c) Die Schwelle einer wenigstens konkretisierten Gefahr | 171 |
| 5. Strenge Eingriffsvoraussetzungen | 172 |
| III. Neues HSOG | 174 |
| 1. Verwendung von Daten im Strafprozessrecht | 174 |
| 2. Merkmale der automatisierten Datenanalyse | 174 |

| | |
|--|-----|
| 3. Bestandteile von automatisierten Analysedaten | 176 |
| 4. Einschränkungen des Datenumfangs bei der automatisierten Datenanalyse | 177 |
| 5. Sicherung der Grundsätze von Zweckbindung und Zweckänderung | 178 |
| a) Rollen und Rechtskonzept | 178 |
| b) Konzept der Kategorisierung und Kennzeichnung personenbezogener Daten | 179 |
| 6. Zugangskontrolle und Protokollierung | 180 |
| 7. Einrichtung und wesentliche Änderung | 181 |
| IV. Zwischenfazit | 181 |
| C. England – Edward Bridges Urteil | 183 |
| I. Sachverhalt | 183 |
| II. The Divisional Court’s judgment | 184 |
| 1. Artikel 8 der EU-Grundrechtecharta | 184 |
| 2. Einhaltung des Verhältnismäßigkeitsgrundsatzes | 185 |
| 3. Überprüfung des Datenschutzes | 186 |
| 4. Diskriminierende Risikoprobleme | 187 |
| III. Ansichten von HIGH COURT | 188 |
| 1. Mangelnde Klarheit der Rechtsvorschriften | 188 |
| 2. Grundsatz der Verhältnismäßigkeitsprüfung | 189 |
| 3. Datenschutzrechtliches Problem der Folgenabschätzung | 190 |
| 4. Dokumentation des Schutzes personenbezogener Daten | 191 |
| 5. Das Risiko von Diskriminierungen | 191 |
| IV. Zwischenfazit | 193 |
| 1. Verletzung der Privatsphäre im öffentlichen Raum | 193 |
| 2. Anforderungen an die Klarheit der gesetzlichen Regelung | 195 |
| 3. Verhältnismäßigkeitsprinzip – Verfahrens- und Organisationsgarantien | 195 |
| 4. Ausschluss von Diskriminierungsrisiken | 196 |
| D. Niederländisches Fall-System SyRI | 197 |
| I. Sachverhalt | 197 |
| II. Die Feststellung des Gerichts | 198 |
| 1. Verstoß gegen die Privatsphäre | 198 |
| 2. Verstoß gegen den Verhältnismäßigkeitsgrundsatz | 200 |
| a) Erhebliche Auswirkungen auf den Risikobericht | 200 |

| | |
|--|-----|
| b) Mangel an Transparenz und Überprüfbarkeit | 201 |
| aa) Mangel an Transparenz | 201 |
| bb) Datenerhebung und -auswertung entsprechen nicht dem Verhältnismäßigkeitsgrundsatz | 201 |
| cc) Diskriminierungsrisiko | 202 |
| dd) Das Gericht kann auch nicht überprüfen | 202 |
| III. Zwischenfazit | 203 |
| 1. Klarheit in Rechtsnormen | 203 |
| 2. Anforderungen an die Transparenzpflichten | 204 |
| 3. Transparenz mindert das Diskriminierungsrisiko | 205 |
| E. Japans Blick | 205 |
| I. N-System-Urteil | 205 |
| 1. Sachverhalt | 205 |
| 2. Urteil | 206 |
| a) Kein Verstoß gegen das Recht auf Bildnis | 206 |
| b) Kein Verstoß gegen das Recht auf Freizügigkeit | 207 |
| c) Kein Verstoß gegen das Recht auf informationelle Selbstbestimmung | 208 |
| II. Japanische Ansicht zum Gesichtserkennungssystem | 209 |
| 1. Vorschläge der Anwaltskammer aus dem Jahr 2016 | 209 |
| a) Anforderungen an rechtliche Beschränkungen | 210 |
| aa) Anforderungen an richterliche Genehmigungen | 210 |
| bb) Beschränkung der Überwachung auf schwere organisierte Verbrechen und Pflicht zur Datenvernichtung | 211 |
| cc) Beschränkung des Datenabgleichs auf Personen, die wegen schwerer, organisierter Kriminalität verurteilt wurden | 211 |
| dd) Regelung zur Löschung von Daten | 211 |
| ee) Gesetzlich ausdrücklich eingeschränkt | 212 |
| b) Einrichtung eines Datenschutzausschusses | 212 |
| c) Veröffentlichung grundlegender Informationen | 212 |
| d) Rechte von Verdächtigen, Beschuldigten und Personen, die sich in ähnlichen Situationen befinden | 213 |
| 2. Vorschläge der Anwaltskammer aus dem Jahr 2021 | 213 |

| | |
|--|-----|
| 3. Bewertung der Probleme von Gesichtserkennungssystemen in Japan | 215 |
| a) Datenerhebungsphase | 217 |
| aa) Klare Definition des Zwecks der Datenerhebung | 217 |
| bb) Gerichtliche Überprüfung der Erfassung von Informationen | 217 |
| b) Informationsverarbeitung und -analyse | 218 |
| aa) Grundsatz der Verhältnismäßigkeit | 218 |
| bb) Menschliche Überprüfung und Ausschluss von irrelevanten Daten | 219 |
| c) Probleme der Datenspeicherung | 220 |
| III. Zwischenfazit | 220 |
| F. Taiwans Blick | 223 |
| I. Untersuchung von Kryptowährungen oder virtuellen Währungen | 225 |
| 1. Überwachung des physischen Geldflusses | 225 |
| 2. Blockchain-Geldflussanalyse-Tool Chainalysis Reactor | 227 |
| 3. Die Voraussetzungen der Verwendung | 229 |
| a) Arten von Fällen | 229 |
| b) Erforderlichkeitsprüfung | 230 |
| 4. Zwischenfazit | 230 |
| II. Überdenken des Einsatzes von künstlicher Intelligenz bei der Strafverfolgung durch technologische Ermittlungsanwendungen | 232 |
| 1. M-AUTO-Fall | 232 |
| a) Urteil | 233 |
| aa) Eingriff in die Privatsphäre | 233 |
| bb) Fehlende Rechtsgrundlage | 234 |
| cc) Eindeutige, gesetzliche Regelungen | 235 |
| b) Die Bewertung für M-AUTO | 236 |
| 2. Entwurf des taiwanesischen Gesetzes zur Ermittlung von Technologie | 237 |
| a) Technologische Überwachung in nicht-physischen Räumen | 237 |
| b) Technologische Überwachung in physischen Räumen | 238 |
| c) Online-Durchsuchung | 239 |
| d) Beschlagnahme von elektromagnetischen Aufzeichnungen | 240 |

| | |
|---|---------|
| e) Rechtsbehelfe und Strafen | 241 |
| f) Kommentar zum Gesetzesentwurf zum Taiwan Technology Investigation Law | 242 |
| G. Zwischenfazit | 243 |
| Kapitel 5: Zusammenfassung der Schlussfolgerungen | 247 |
| A. Zusammenfassung | 247 |
| B. Vorschläge | 248 |
| I. Eine gewisse objektive Tatsache als Voraussetzung | 248 |
| II. Spezifische Verbrechen | 250 |
| III. Notwendigkeit des Richtervorbehalts | 251 |
| IV. Verhältnismäßigkeit | 253 |
| V. Menschliche Autonomie und Kontrolle | 255 |
| VI. Risikobewertung und Datenschutzmanagement | 256 |
| 1. Unabhängige Risikobewertung | 256 |
| 2. Datenschutz-Risikomanagement | 257 |
| a) Klare Definition der Zwecke der Datenerhebung und -verwendung | 257 |
| b) Benachrichtigung | 258 |
| VII. Gewährleistung von Transparenz | 258 |
| VIII. Rechtsbehelfe | 259 |
| IX. Erfassung und Verfolgung von Verantwortlichkeiten | 260 |
| X. Strenge Regeln für den Ausschluss unzulässiger Beweismittel | 260 |
| Literaturverzeichnis | 263 |