

Gutachterliche Stellungnahme für den Verkehrsausschuss des Deutschen Bundestages

Sachverständigen-Anhörung vom 23. Februar 2026

Deutscher Bundestag
Verkehrsausschuss
Ausschussdrucksache
21(15)56-F
vom 19.02.2026
öff. Anhörung 23.02.2026

Gesetzesentwurf der Bundesregierung
Entwurf eines Fünften Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer
straßenverkehrsrechtlicher Vorschriften
BT-Drs. 21/3505

und dem

Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN
Parken fair gestalten – Nachhaltig, digital und sozial gerecht
BT-Drs. 21/3610

19. Februar 2026

Univ.-Prof. Dr. Dirk Heckmann

Lehrstuhl für Recht und Sicherheit der Digitalisierung
Technische Universität München

Ass. iur. Joanna Klauser, wissenschaftliche Referentin (bidt)
Ass. iur. Pascal Bronner, wissenschaftlicher Mitarbeiter (TUM)

Inhalt der Stellungnahme

A.	Einleitung	3
B.	Zusammenfassung	3
C.	Digitaler Führerschein	6
I.	Bewertung der technischen Zugangsvoraussetzungen, § 2d Abs. 1, 2 StVG-E	6
II.	Datenschutzrechtliche Rechtsgrundlagen, § 2d Abs. 4–6 StVG-E	7
1.	Rechtsgrundlage für die Verarbeitung zur Generierung des digitalen Führerscheins.....	7
2.	Einwilligung zur Verarbeitung des Lichtbilds der Antragsteller.....	8
3.	Rechtsgrundlage für die Verarbeitung zum Betrieb des Anwenderprogramms	10
III.	Technischer Standard und Interoperabilität, § 2d Abs. 3 StVG-E	10
IV.	Praxisgerechtigkeit	11
1.	Schnittstellen für private Mobilitätsdienstleister	11
2.	Offline-Kontrollen und technischer Ausfall	11
V.	Nachweis und Ausschluss, § 2 Abs. 1a, 1b StVG-E: Aktualität beim Vollzug	12
VI.	Fazit und Handlungsempfehlungen.....	12
D.	Digitale Parkraumüberwachung.....	13
I.	Verfassungsrechtliche Maßstäbe	14
1.	Anwendbare Grundrechtsordnung.....	14
2.	Grundrechtsrelevante Vorgänge	14
3.	Besonders relevante Rechtsprechung.....	15
a)	Kfz-Kennzeichenkontrolle	16
b)	HessenDATA	17
c)	Videoüberwachung	17
d)	Fotografische Erfassung von Geschwindigkeitsverstößen	18
II.	Bewertungen und Empfehlungen.....	18
1.	Eingabepflicht des Kfz-Kennzeichens, § 63g Abs. 1 StVG-E	18
2.	Mobile optisch-elektronische Einrichtungen (Videokontrollen), § 63g Abs. 2 und 3 StVG-E	19
a)	Anlasslosigkeit und Streubreite der Maßnahmen.....	21
b)	Möglichst geringe Datenerfassung.....	21
c)	Automatische Datenverarbeitung.....	22
d)	Einschüchterungseffekte	23
III.	Sekundärrechtliche Vorgaben des Unionsrechts	24
IV.	Abschließende Handlungsempfehlungen	25
E.	Die Gutachterinnen und Gutachter	27

A. Einleitung

Der Entwurf eines Fünften Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer straßenverkehrsrechtlicher Vorschriften (BT-Drs. 21/3505), den es hier sachverständig zu bewerten gilt, löst ein politisches Versprechen ein, das im Koalitionsvertrag der aktuellen Bundesregierung verankert wurde. Dabei zieht sich die Digitale Transformation der Verwaltung wie ein roter Faden durch die Vorschläge zur Reform bzw. Modernisierung des Straßenverkehrsrechts. Digitalisierung kann hierbei unter zwei Perspektiven betrachtet werden: Zum einen als Umstellung von straßenverkehrsrechtlich relevanten Verfahrensbestandteilen in eine digitale Form einschließlich der hierfür erforderlichen Datenerhebung, Datenverarbeitung und Datenübermittlung, zum anderen als Ermächtigung zur Nutzung digitaler Technologien für Zwecke einer effizienten Gewährleistung von Verkehrssicherheit. Oder anders ausgedrückt: Es geht sowohl um Verwaltungsverfahrenrecht als auch um materielles Sicherheitsrecht.

Die insoweit im Gesetzentwurf vorgeschlagenen Änderungen und Ergänzungen sind vielfältig und konnten in der knappen Frist zur Erstellung einer gutachterlichen Stellungnahme nicht umfassend rechtlich untersucht und gewürdigt werden. Um aber hilfreiche Hinweise für das weitere Gesetzgebungsverfahren geben zu können, greift die Stellungnahme aus jeder der vorgenannten Perspektiven eine Vorschrift exemplarisch auf und analysiert diese, um konkrete Handlungsempfehlungen zu geben. Das ist zum einen § 2d StVG-E (digitaler Führerschein), zum anderen § 63g StVG-E (digitale Parkraumüberwachung).

B. Zusammenfassung

1. Der Entwurf eines Fünften Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer straßenverkehrsrechtlicher Vorschriften (BT-Drs. 21/3505) ist insgesamt sehr zu begrüßen. Die Umsetzung der dort zur Änderung und Ergänzung vorgeschlagenen Vorschriften wird dafür sorgen, dass wichtige Teile des Verfahrensrechts und des materiellen Rechts im Verkehrswesen auf einen zeitgemäßen Stand gehoben werden. Die Schaffung von Rechtsgrundlagen für den Einsatz digitaler Anwendungen ist vielfach datenschutzrechtlich geboten und sorgt überdies für Rechtssicherheit. Insoweit lassen sich auch Eingriffe in das Recht auf informationelle Selbstbestimmung verfassungsrechtlich rechtfertigen.

2. Die Einführung des „Digitalen Führerscheins“ (§ 2d StVG-E) fügt sich nahtlos in die digitale Agenda ein, wonach Verwaltungsvorgänge zunehmend digital abgebildet werden sollen. Zu diesen Vorgängen zählt auch das polizeiliche Verlangen nach Überprüfung des Bestehens einer Fahrerlaubnis der kontrollierten Person, etwa im Rahmen einer Verkehrskontrolle oder der Aufnahme eines Verkehrsunfalls. Während diesem Kontrollbedürfnis bislang durch das Vorzeigen des mitgeführten, quasi analogen Führerscheins

Rechnung getragen wurde, kann ein Datenabgleich zukünftig durch den Digitalen Führerschein erfolgen, der in die technisch hierfür geeignete Applikation auf einem Smartphone integriert wird. Angesichts der Tatsache, dass 82 % der hier relevanten Bevölkerung in Deutschland über ein Smartphone verfügt und dort vielfach andere Berechtigungen (wie etwa das Deutschlandticket, Banking-Apps oder E-Government-Fachanwendungen) speichert, erscheint die Einführung des Digitalen Führerscheins als überfälliger Schritt.

3. Wichtig ist in diesem Zusammenhang, dass Datenschutz und Datensicherheit insbesondere zur Vermeidung missbräuchlicher Zugriffe gewährleistet sind und die Nutzung des Digitalen Führerscheins in den Einsatzszenarien praktikabel ist. Außerdem dürfen jene Personen, die diesen nicht nutzen können oder wollen, in der Kontrollsituation nicht diskriminiert werden (Wahlfreiheit, ob man die analoge oder digitale Variante des Führerscheins nutzen will). All dem wurde im Entwurf Rechnung getragen.

4. Hinzuweisen ist ergänzend auf die folgenden Punkte:

- Entgegen der Gesetzesbegründung ist hinsichtlich minderjähriger Antragsteller für den Führerschein nicht auf Art. 8 DSGVO, sondern vielmehr auf die individuelle Einsichtsfähigkeit des minderjährigen Führerscheininhabers abzustellen. Denn Art. 8 DSGVO ist nur auf „Dienste der Informationsgesellschaft“ anzuwenden; ein solcher Dienst liegt hier nicht vor. Im Ergebnis ändert sich aber nichts an der datenschutzrechtlichen Zulässigkeit dieses Verfahrens.
- Es ist begrüßenswert, dass die Implementierung des Digitalen Führerscheins in die „EUId-Brieftasche“ erfolgen soll, die ein EU-weit harmonisiertes Identifizierungsmittel auf dem Smartphone darstellen und voraussichtlich ab Anfang 2027 in allen Mitgliedstaaten verfügbar sein wird.
- Die Praxistauglichkeit des Digitalen Führerscheins hängt auch davon ab, dass dieser nicht nur bei staatlichen Kontrollen, sondern auch im privaten Rechtsverkehr, etwa bei Autovermietungen zum Einsatz kommen kann. Das ist technisch sicherzustellen.
- Zu begrüßen ist, dass der Gesetzgeber auch die Situation eines technischen Ausfalls des Digitalen Führerscheins mitbedacht hat. Bei der Prüfung einer etwaigen Verkehrsordnungswidrigkeit ist auch zu berücksichtigen, inwieweit der Betroffene den Grund für den Ausfall zu vertreten hat; ggf. ist sogar von einem Bußgeld abzu sehen.
- Für einen effektiven und rechtskonformen Vollzug ist sicherzustellen, dass der digitale Führerschein offline nutzbar ist und zeitnah aktualisiert wird, sodass Sperren oder Entziehungen der Fahrerlaubnis zuverlässig und aktuell abgebildet werden.

5. Die Neuregelung der digitalen Parkraumüberwachung (§ 63g StVG-E) trägt dem Umstand Rechnung, dass aufgrund eines zunehmenden Fachkräftemangels und knapper Verwaltungsressourcen notwendige Kontrollen des ruhenden Verkehrs zukünftig nicht mehr

ohne Weiteres gewährleistet werden können. Dass zur Lösung an die Entwicklung digitaler Kontrolltechnologien gedacht und dies wiederum durch die Schaffung von Rechtsgrundlagen rechtsstaatlich abgesichert wird, ist generell zu begrüßen. Der Gesetzentwurf deckt die notwendigen rechtlichen Anforderungen ab, er erscheint insbesondere mit Blick auf die betroffenen Grundrechte der Verkehrsteilnehmer ausgewogen. Gleichwohl ist die eine oder andere Detailregelung erörterungswürdig. Das hängt damit zusammen, dass das Bundesverfassungsgericht in seiner fast 20-jährigen Rechtsprechung zum IT-Einsatz im Sicherheitsrecht strenge Anforderungen an den Grundrechtsschutz aufgestellt hat. Weil es zu dem hier konkret geplanten Einsatzszenario aber noch keine höchstrichterliche Entscheidung gibt, muss der Gesetzgeber eine Risikoabwägung vornehmen: Will man durch Korrekturen im Detail einen verfassungsrechtlich sicheren Weg gehen oder notfalls riskieren, dass das Bundesverfassungsgericht in dem zu erwartenden verfassungsgerichtlichen Verfahren weitere Grenzen zieht. Dies betrifft die folgenden Punkte:

- Die Abschwächung der Eingriffstiefe bzw. Streubreite durch Ausgestaltung als stichprobenartige Kontrolle § 63 Abs. 2 und 3 StVG-E sollte beibehalten werden.
- Die Fassung in § 63g Abs. 2 S. 1 Nr. 1 und Abs. 3 S. 2 Nr. 1 StVG-E, wonach Personen und Kfz-Kennzeichen nach dem „Stand der Technik“ „unkennlich“ zu machen seien, könnte durch die Formulierung „irreversibel unkenntlich“ verstärkt werden, um eine Re-Identifizierung auszuschließen.
- Zusätzlich sollte die technische Anforderung an die „mobile optisch-elektronische Einrichtung“ präzisiert werden, wonach die Erfassung von Personen durch Einstellung des Erfassungswinkels weitgehend ausgeschlossen ist. Weil Videoaufnahmen von unbeteiligten Menschen einen Grundrechtseingriff darstellen, ist dies auch im Gesetzestext aufzunehmen.
- Die Datennutzungsverbote in § 63g Abs. 6 StVG-E sind zur Vermeidung von Einschüchterungseffekten essenziell und sollten beibehalten werden.
- Darüber hinaus ist in diesem Kontext zu erwägen, den Einsatz von Videokontrollen für den Zeitraum von grundrechtlich geschützten Versammlungen (Demonstrationen) auszusetzen, um der auch vom BVerfG attestierten überragenden Bedeutung der Versammlungsfreiheit Rechnung zu tragen.

C. Digitaler Führerschein

Die vorliegende Initiative zur Ergänzung des Straßenverkehrsgesetzes und anderer straßenverkehrsrechtlicher Vorschriften zur Schaffung einer Rechtsgrundlage für die Etablierung des digitalen Führerscheins als zentralem Baustein der Nationalen Digitalstrategie wird ausdrücklich begrüßt. Damit verfolgt der Gesetzgeber das legitime und längst überfällige Ziel, die Nachweispflichten im Straßenverkehr an die Lebensrealität einer digitalisierten Gesellschaft anzupassen und zugleich Effizienzpotenziale innerhalb der öffentlichen Verwaltung zu steigern. Die Einführung erfolgt ebenso im Einklang mit Art. 5 der RL 2025/2205. Die Einführung eines digitalen Führerscheins fügt sich überzeugend in den übergeordneten Kontext der Verwaltungsdigitalisierung ein.¹ Dabei hat sich die Erwartungshaltung der Bürgerinnen und Bürger im Zeitalter der Digitalisierung nachhaltig verändert: Verwaltung wird zunehmend nicht mehr primär als papiergebundene Präsenzverwaltung wahrgenommen, sondern als digital zugänglicher Dienstleister. Vor diesem Hintergrund erscheint es folgerichtig, klassische hoheitliche Nachweisdokumente – wie den Führerschein – rechts- und datensicher in digitale Nutzungsformen zu überführen.

I. Bewertung der technischen Zugangsvoraussetzungen, § 2d Abs. 1, 2 StVG-E

Nach § 2d Abs. 1 StVG-E können Inhaber von Führerscheinen, die ab dem 1.1.1999 als Kartenführerschein ausgestellt worden sind, die Erstellung eines digitalen Führerscheins beim Kraftfahrt-Bundesamt (KBA) beantragen. Ausweislich des Wortlauts der Regelung ist die Beantragung des digitalen Führerscheins optional. Der analoge Kartenführerschein soll nicht ersetzt, sondern ergänzt werden.² Neben dem Ausstellungsdatum knüpft § 2d Abs. 2 StVG-E die Erstellung eines digitalen Führerscheins an ein geeignetes mobiles Endgerät³ sowie die nach § 18 PAuswG optionale Nutzung der eID-Funktion des Personalausweises. Aus verwaltungsdigitalisierenden Maßnahmen darf aufgrund unterschiedlicher technischer Zugangsvoraussetzungen indes keine (ungerechtfertigte) Ungleichbehandlung nach Art. 3 Abs. 1 GG resultieren.⁴ Die Voraussetzungen für die Beantragung und Erstellung eines digitalen Führerscheins nach § 2d Abs. 1, 2 StVG-E sind im Hinblick auf eine **(potenzielle) Ungleichbehandlung** allerdings **verhältnismäßig**:

¹ Der digitale Führerschein soll wie bereits aktuell der digitale Fahrzeugschein (Zulassungsbescheinigung Teil I) in die i-Kfz-App des Kraftfahrtbundesamtes (KBA) integriert werden, nach aktuellem Stand ist dies Ende 2026 geplant, s. <https://www.tagesschau.de/inland/innenpolitik/digitaler-fuehrerschein-102.html> (zuletzt abgerufen am 18.2.2026).

² S. hierzu die Begründung, BT-Drs, 21/3505, S. 21.

³ Zudem ist die aktuelle i-Kfz-App an bestimmte Betriebssysteme gebunden (z.B. iOS ab Version 17 und Android ab Version 12) m s. <https://www.bmv.de/goto?id=176616> (zuletzt abgerufen am 18.2.2026). Auf Huawei-Geräten sowie älteren Motorola-Geräten ist die i-Kfz-App aktuell nach Angaben des KBA nicht nutzbar, vgl. https://www.kba.de/DE/Themen/ZentraleRegister/iKfz_App/DFZ/dfz_node.html (zuletzt abgerufen am 18.2.2026).

⁴ So generell bereits Heckmann, MMR 2006, 3 (6).

- Die Beschränkung der Antragsberechtigung auf Inhaber eines nach dem 1.1.1999 ausgestellten Kartenführerscheins begründet sich damit, dass ausweislich § 2d Abs. 5 StVG-E zur Generierung des digitalen Führerscheins eine Erfassung der Daten im Zentralen Fahrerlaubnisregister (ZFER) erforderlich ist, was ausschließlich nach dem 1.1.1999 ausgestellte Führerscheine erfasst.⁵ Hieraus könnte ein nicht zu rechtfertigender faktischer Umtauschzwang für Inhaber älterer Führerscheine resultieren. Zum einen ist allerdings der **sukzessive Umtausch von Führerscheinen**, die vor dem 19.1.2013 ausgestellt worden sind, in Umsetzung von Art. 3 Nr. 3 RL 2006/12/EG zum Schutz vor Fälschungen nach § 24a Abs. 2 S. 1 i.V.m. Anlage 8e zur FeV bis zum 19.1.2033 ohnehin rechtlich verbindlich. Zum anderen bleibt der digitale Führerschein ausweislich des Gesetzesentwurfs optional und führt hierdurch nicht zu faktischen Nachteilen bei Kontrollen, Dienstleistungen oder Mobilitätsangeboten. Dies ist zumindest bis zum Ablauf der Umtauschfrist für alle Führerscheine sicherzustellen.
- Auch die zwingende Voraussetzung, dass beim Antragsteller ein **mobiles Endgerät** (mit einem bestimmten Betriebssystem) vorhanden sein muss, führt im Hinblick auf digital wenig affine Bevölkerungsgruppen sowie einkommensschwächere Personen in einem teilhaberelevanten Bereich ein Ungleichbehandlungsrisiko mit sich. Sofern sichergestellt ist, dass bei Kontrollen, Dienstleistungen oder Mobilitätsangeboten der analoge Führerschein praktisch gleichwertig ist und der digitale Führerschein wie im Entwurf des Gesetzes vorgesehen nur eine ergänzende Option darstellt, ist dies unbedenklich.

II. Datenschutzrechtliche Rechtsgrundlagen, § 2d Abs. 4–6 StVG-E

Mit der Generierung und dem Betrieb des digitalen Führerscheins ist die Verarbeitung personenbezogener (Führerschein-)Daten der jeweiligen Antragsteller und Inhaber verbunden. Aufgrund des Eingriffs in den Schutzbereich der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG bzw. Art. 8 GRCh ist daher eine tragfähige Rechtsgrundlage für die Verarbeitung erforderlich. Aus datenschutzrechtlicher Perspektive ist die Etablierung dahingehender Rechtsgrundlagen in den § 2d Abs. 4 – 6 StVG-E zu begrüßen. Jedoch müssen die Vorgaben der DSGVO sowie für das KBA als Bundesoberbehörde die des BDSG⁶ beachtet werden.

1. Rechtsgrundlage für die Verarbeitung zur Generierung des digitalen Führerscheins

Nach **§ 2d Abs. 5 S. 1 StVG-E** darf das KBA als verantwortliche Stelle zur **Generierung** des digitalen Führerscheins aus dem ZFER die personenbezogenen Daten nach § 2d Abs.

⁵ Vgl. hierzu auch https://www.kba.de/DE/Themen/ZentraleRegister/ZFER/zfer_node.html (zuletzt abgerufen am 18.2.2026).

⁶ Das BDSG findet nach § 1 Abs. 1 Nr. 1 BDSG auf die Verarbeitung personenbezogener Daten durch öffentliche Stellen des Bundes Anwendung, wozu die Behörden des Bundes gehören, s. auch Gola/Reif, in: Gola/Heckmann, DSGVO/BDSG, § 1 BDSG Rn. 4.

4 StVG-E verarbeiten, wozu mit Ausnahme der Unterschrift „alle Daten eines deutschen Führerscheins“ gehören. Ausweislich § 2d Abs. 5 S. 2 StVG-E ist auch das Lichtbild nicht von dieser gesetzlichen Grundlage zur Erfüllung eines öffentlichen Interesses i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2, 3 DSGVO bzw. § 3 BDSG erfasst. Mit der abschließenden Begrenzung auf die Daten des Führerscheins⁷ ohne die Unterschrift und somit alle fahrerlaubnisrelevanten, erforderlichen personenbezogenen Daten erfolgt eine im Sinne der Datenminimierung und Zweckbindung **begrüßenswerte Eingrenzung** der zu verarbeitenden Datenkategorien.

2. Einwilligung zur Verarbeitung des Lichtbilds der Antragsteller

Das für die **Erstellung** des digitalen Führerscheins erforderliche Lichtbild darf **nach § 2d Abs. 5 S. 2 StVG-E** nur mit Einwilligung der Antragsteller durch das KBA bei der ausstellenden Pass- und Personalausweisbehörde (i.V.m. § 22a Abs. 2 S. 6 Nr. 1 PassG bzw. § 25 Abs. 2 S. 5 PAuswG) oder bei den zentralen Lichtbildbeständen der Länder (soweit landesrechtlich abgesichert) abgerufen und zur Generierung des digitalen Führerscheins weiterverarbeitet werden. In der Gesetzesbegründung hierzu wird ausgeführt, dass die Vorgaben der DSGVO, namentlich der Art. 4 Nr. 11 i.V.m. Art. 7 DSGVO sowie (im Falle minderjähriger Antragsteller) Art. 8 DSGVO einzuhalten sind.⁸ Als genuiner Ausdruck der informationellen Selbstbestimmung des Individuums ist die Einwilligung dabei insbesondere informiert, bestimmt und freiwillig zu erteilen.

- Die Einwilligung muss nach Maßgabe des Art. 4 Nr. 11 DSGVO informiert erfolgen. Die **Informiertheit** setzt voraus, dass sich die Antragsteller dem Umfang und die Tragweite der Verarbeitung ihrer Lichtbilder (Abruf und Generierung) bewusst sind. Das KBA hat daher im Rahmen der Gestaltung der Antragstellung die Antragsteller umfassend über die Einwilligung aufzuklären. Hierbei hat es sich an den ohnehin zu beachtenden Informationspflichten nach Art. 13, 14 DSGVO und den Anforderungen des Art. 12 DSGVO an eine präzise, transparente, verständliche und leicht zugängliche Form und eine klare und einfache Sprache sowie eine barrierefreie und adressatengerechte Information zu orientieren. Insbesondere ist klarzustellen, dass sich die Einwilligung nur auf den Abruf und die Verarbeitung des Lichtbildes erstreckt, während die anderen Datenkategorien bei Antragstellung auf Basis einer gesetzlichen Grundlage verarbeitet werden. Zudem ist klarzustellen, dass das Lichtbild nicht nur für den Abruf und die Generierung des digitalen Führerscheins verarbeitet wird, sondern auch anschließend (soweit erforderlich) für den Betrieb auf Basis einer gesetzlichen Grundlage nach § 2d Abs. 6 StVG-E verarbeitet werden kann. Schließlich ist auf die jederzeitige Möglichkeit des

⁷ Die für den Führerschein erforderlichen Daten sind insb. in § 25 Abs. 1 i.V.m. Anlage 8 zur FeV sowie § 25 Abs. 3 i.V.m. Anlage 9 zur FeV aufgeführt.

⁸ S. hierzu die Begründung, BT-Drs, 21/3505, S. 46.

Widerrufs i.S.d. Art. 7 Abs. 3 DSGVO hinzuweisen. Nur so ist den Antragstellern die Tragweite ihrer Einwilligung bewusst.

- Außerdem ist das Merkmal der **Freiwilligkeit** zu beachten. Dies setzt voraus, dass die Einwilligung nicht mit Zwang herbeigeführt wird und die betroffenen Personen eine echte Wahl hinsichtlich der Einwilligung in die Datenverarbeitung besitzen. Grundsätzlich indiziert die Machtasymmetrie zwischen Behörden (KBA als Bundesoberbehörde) und betroffenen Personen (Antragsteller des digitalen Führerscheins) die Unfreiwilligkeit einer Einwilligung,⁹ ohne dass aber die Freiwilligkeit von vornherein ausgeschlossen ist.¹⁰ Da es sich bei dem Abruf des Lichtbildes und der anschließenden Generierung des digitalen Führerscheins um ein Element der Leistungsverwaltung handelt,¹¹ das optional als Nachweis für die Fahrerlaubnis neben den analogen Führerschein tritt, kann das Merkmal der Freiwilligkeit vorliegend erfüllt sein. Insbesondere initiiert der Antragsteller das Antragsverfahren selbst. Ohne das Lichtbild kann die Identitätsfunktion des digitalen Führerscheins nicht erbracht werden, weshalb auch mit Blick auf Art. 7 Abs. 4 DSGVO die Freiwilligkeit nicht ausgeschlossen ist. Es ergeben sich wegen des analogen Führerscheins aus der Ablehnung einer Einwilligung keine rechtlichen Nachteile für den jeweiligen Führerscheininhaber. Hinzu tritt der bereits unter I. angesprochene Punkt, dass die Entscheidung zur Verweigerung der Einwilligung bei Kontrollen, Dienstleistungen oder Mobilitätsangeboten nicht zu faktischen Nachteilen bzw. zu sozialem Druck führen darf, wodurch die Freiwilligkeit der Einwilligung ebenfalls nicht gegeben wäre.¹² Essenziell ist daher die Sicherstellung der Gleichwertigkeit des analogen zum digitalen Führerschein.
- Entgegen der Gesetzesbegründung ist hinsichtlich **minderjähriger Antragsteller** für den Führerschein nicht auf Art. 8 DSGVO, sondern vielmehr auf die individuelle Einsichtsfähigkeit des minderjährigen Führerscheininhabers abzustellen. Denn Art. 8 DSGVO ist nur auf „Dienste der Informationsgesellschaft“ anzuwenden, die sich nach Art. 4 Nr. 25 DSGVO i.V.m. Art. 1 Nr. 1 lit. b RL (EU) 2015/1535 als (i.d.R.) gegen Entgelt (...) im Fernabsatz (...) erbrachte Dienstleistung definiert. Zwar kann dieses Entgelt bei datengetriebenen Geschäftsmodellen auch einzig in der Hingabe personenbezogener Daten zu sehen sein,¹³ bei der Generierung eines digitalen Führerscheins zur unentgeltlichen Nutzung sowie zu altruistischen Zwecken im Sinne einer effektiven Verwaltungsdigitalisierung ist hiervon aber nicht

⁹ Erwägungsgrund 43 S. 1 zur DSGVO. Grds. hierzu *Klement*, in: Simitis/Hornung/Spiecker gen. Döhmman, Datenschutzrecht, DSGVO Art. 7 Rn. 44 ff.

¹⁰ S. EDSA, Leitlinien 05/2020 (v.1.1) v. 4.5.2019, S. 9 Rn. 17 mit weiteren Bsp.

¹¹ *Stemmer*, in: Wolff/Brink/von Ungern-Sternberg, BeckOK Datenschutzrecht (54. Ed., 1.11.2025), Art. 7 Rn. 54; *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 7 Rn. 57.

¹² S. hierzu im Kontext der Corona-Warn-App auch *RuscheMeier*, ZD 2020, 618 (620).

¹³ Vgl. *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 8 Rn. 18.

auszugehen.¹⁴ Daher ist bei minderjährigen Führerscheininhabern die individuelle Einsichtsfähigkeit maßgeblich. Während ab Vollendung des 16. Lebensjahres (und damit für alle Führerscheininhaber der Klasse B im Rahmen des „Begleiteten Fahrens ab 17“) eine Einsichtsfähigkeit anzunehmen ist,¹⁵ ist diese vor Vollendung des 16. Lebensjahres (und damit etwa auch in den Führerscheinklassen AM, A1 und Mofa) von der – ohnehin zu prüfenden – individuellen Einsichtsfähigkeit abhängig, die bei Verneinung die Einwilligung des **Trägers der elterlichen Verantwortung** zu ihrer Wirksamkeit bedarf. Gerade hinsichtlich der angeführten Führerscheinklassen ist dieser Umstand bei der **Online-Antragstellung** zu berücksichtigen und technisch-organisatorisch entsprechend zu implementieren.

- Es ist sicherzustellen, dass bei einem **Widerruf** der Einwilligung nach Art. 7 Abs. 3 DSGVO nach Maßgabe des Art. 17 Abs. 1 lit. b DSGVO die personenbezogenen Daten der betroffenen Person, vorbehaltlich des Art. 17 Abs. 3 DSGVO unverzüglich gelöscht werden.

3. Rechtsgrundlage für die Verarbeitung zum Betrieb des Anwenderprogramms

Nach **§ 2d Abs. 6 StVG-E** dürfen die nach § 2d Abs. 4, 5 StVG-E zur Erstellung des digitalen Führerscheins erhobenen Daten (sowohl die Daten auf Basis von § 2d Abs. 5 S. 1 StVG-E als auch die Daten auf Basis von § 2d Abs. 5 S. 2 StVG-E) durch das KBA auch während des **Betriebs** des Anwenderprogramms verarbeitet werden, soweit dies hierfür erforderlich ist. Dies stellt eine gesetzliche Grundlage zur Erfüllung eines öffentlichen Interesses i.S.d. Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2, 3 DSGVO bzw. § 3 BDSG dar. Bei der Datenverarbeitung im Rahmen dieser Rechtsgrundlage sind nicht nur die Grundsätze der Datenminimierung und Zweckbindung in besonderem Maße zu berücksichtigen, vielmehr sind die Zugriffe auch i.S.d. Art. 30 DSGVO zu protokollieren.

III. Technischer Standard und Interoperabilität, § 2d Abs. 3 StVG-E

Bei der Entwicklung eines technischen Standards über die Form der Antragstellung sowie die technische Ausgestaltung des digitalen Führerscheins durch das KBA nach § 2d Abs. 3 StVG-E ist es wichtig, dass die eben erörterten **datenschutzrechtlichen Anforderungen** berücksichtigt werden. Zudem ist es bei der Entwicklung eines technischen Standards essenziell, die Anforderungen an die **Datensicherheit** sowie die **IT-Sicherheit** innerhalb dieser Standards zu etablieren. Die Beteiligung des Bundesamts für Sicherheit in der Informationstechnik (BSI) bei der Entwicklung dieser Standards ist daher positiv zu beurteilen. Dies umfasst im Hinblick auf die Datensicherheit die Festlegung von Maßnahmen

¹⁴ S. so im Kontext der Corona-Warn-App schon *Heckmann/Paschke*, in: Ehmann/Selmayr, DSGVO, Art. 8 Rn. 18 sowie *Taeger*, in: Taeger/Gabel, DSGVO – BDSG – TDDDG, Art. 8 DSGVO Rn. 18.

¹⁵ I. Erg. auch *Frenzel*, in: Paal/Pauly, DS-GVO BDSG, Art. 8 DSGVO Rn. 9; *Buchner/Kühling*, in: Kühling/Buchner, DS-GVO BDSG, Art. 8 DSGVO Rn. 19.

zur Datenminimierung und Zweckbindung, dabei vor allem das Verbot der Weiterverwendung außerhalb der Führerschein-Identitätsfunktion, die Möglichkeit der selektiven Offenlegung erforderlicher Merkmale, Zugriffs- und Berechtigungs- sowie Löschkonzepte. Der Standard hat im Sinne der IT-Sicherheit zudem die sichere und verschlüsselte Speicherung auf dem Endgerät sowie eine Multi-Faktor-Authentifizierung unter Einbindung der Authentifizierungsfunktionen des Smartphones zu beinhalten. Es ist begrüßenswert, dass mit dem technischen Standard in § 2d Abs. 3 S. 1 StVG-E die Implementierung des digitalen Führerscheins in die „EUId-Brieftasche“ nach Art. 5a Abs. 1 eIDAS VO 2.0 intendiert wird, die ein EU-weit harmonisiertes Identifizierungsmittel auf dem Smartphone darstellen und voraussichtlich ab Anfang 2027 in allen Mitgliedstaaten verfügbar sein wird.¹⁶ Auch die Sicherstellung der Interoperabilität zwischen der i-Kfz-App und der EUId-Brieftasche hat die erörterten Aspekte der Daten- und IT-Sicherheit zu gewährleisten.

IV. Praxisgerechtigkeit

1. Schnittstellen für private Mobilitätsdienstleister

Mit der Einführung des digitalen Führerscheins wird auch die künftig erleichterte Nutzung von privaten Mobilitätsdienstleistern wie Carsharing-Anbietern intendiert.¹⁷ Hierbei ist einerseits die Interoperabilität der i-Kfz-App mit den Authentifizierungs- und Prüfungsmechanismen der Mobilitätsdienstleister sicherzustellen. Andererseits ist sicherzustellen, dass der analoge Führerschein auch beim Angebot von privaten Dienstleistern eine gleichwertige Alternative ohne jegliche Nachteile verbleibt.

2. Offline-Kontrollen und technischer Ausfall

Vor dem Hintergrund eines nachhaltigen und diskriminierungsfreien Rechtsvollzugs muss sichergestellt werden, dass der digitale Führerschein im Rahmen von Führerscheinkontrollen auch **offline** nutzbar ist und sich daraus keine nachträglichen Belastungen, Verzögerungen oder Sanktionen ergeben. Sofern das Endgerät **technisch ausfällt** oder aufgrund eines **leeren Akkus** der digitale Nachweis nicht möglich ist und auch der analoge Führerschein nicht mitgeführt wird ist es zunächst sachgerecht, dass dieselben Rechtsfolgen wie bei der Nichtmitführung des analogen Führerscheins gelten. Dies stellen die Änderungen zu § 4 FeV-E sowie § 75 FeV-E sicher. Der Grund des technischen Ausfalls ist im Rahmen des Sorgfaltsmaßstabes eines Ordnungswidrigkeiten-Tatbestandes jedoch hinreichend zu würdigen.

¹⁶ Hierzu allg. Heckmann/Rachut, in: Heckmann/Paschke, jurisPK Internetrecht (Stand: 14.1.2026), Kap. 5 Rn. 158 ff.

¹⁷ Vgl. <https://www.bundesregierung.de/breg-de/aktuelles/kabinett-digitaler-fuehrerschein-2392320> (abgerufen am 18.2.2025).

V. Nachweis und Ausschluss, § 2 Abs. 1a, 1b StVG-E: Aktualität beim Vollzug

§ 2 Abs. 1a S. 1 StVG-E, § 4 Abs. 2a S. 1 FeV-E und die Begründung hierzu sehen vor, dass der **digitale Führerschein** i.S.d. § 2d StVG-E ergänzend als **Nachweis des Führscheins** (nicht der Fahrerlaubnis) fungiert. § 2 Abs. 1b StVG-E sieht zudem vor, dass der Nachweis des Führscheins in bestimmten Fällen (z.B. wirksames Fahrverbot nach § 44 StGB, Erlöschen der Fahrerlaubnis und gerichtlicher Entzug nach § 69 Abs. 1, Abs. 3 S. 1 StGB, vorläufiger Entzug der Fahrerlaubnis nach § 111a Abs. 1 StPO oder weitere behördliche Maßnahmen aufgrund derer der Führerschein sich nicht im Besitz des Inhabers befindet) ausgeschlossen ist. Inhaltsgleich aber mit eindeutigerer Formulierung findet sich ein derartiger Ausschluss auch in § 4 Abs. 2b FeV-E.¹⁸ Da der digitale Führerschein als Nachweis des analogen Führscheins fungiert und dieser als Rechtsfolge der jeweiligen in den Auschlussstatbeständen genannten behördlichen Maßnahmen ebenfalls von seinem Inhaber körperlich getrennt werden soll, erscheint dies konsequent. Allerdings ist unklar, weshalb der selbstverständliche Ausschluss des Nachweises ausdrücklich nur für den digitalen Führerschein geregelt wird. Vielmehr lässt sich hieraus die Vermutung ableiten, dass eine **Aktualisierung** des digitalen Führscheins hinsichtlich fahrerlaubnisbeschränkender Maßnahmen in Echtzeit nicht vorgesehen ist. § 28 Abs. 4 i.V.m. Abs. 3 Nr. 9 StVG sehen etwa eine Datenübermittlung (nach § 28 Abs. 4 S. 2 i.V.m. § 30a Abs. 2 bis 4 StVG ggf. im Wege der Datenfernübertragung) von Gerichten, Staatsanwaltschaften und anderen Behörden an das Fahreignungsregister des KBA weiterhin lediglich hinsichtlich der – physischen – Beschlagnahme, Sicherstellung und Verwahrung vor. Sowohl vor dem Hintergrund des Rechtsvollzugs bei Kontrollen vor dem Hintergrund der steigenden Zahl des Fahrens ohne Fahrerlaubnis¹⁹ als auch im Hinblick auf die Nutzung des Führscheins im Rahmen von Dienstleistungen oder Mobilitätsangeboten wird die Funktionalität des digitalen Führscheins ohne Aktualität stark eingeschränkt. Da der digitale Führerschein an das ZFER gekoppelt ist,²⁰ ist rechtlich und technisch dafür zu sorgen, dass die entsprechenden Informationen (z.B. als Sperrvermerk) aktuell auf dem Smartphone verfügbar sind.

VI. Fazit und Handlungsempfehlungen

Die Digitalisierung des Führscheins wird im Sinne einer effektiven Verwaltungsdigitalisierung ausdrücklich begrüßt. Aus den ausgeführten Erwägungen lassen sich die folgenden zentralen Handlungsempfehlungen ableiten:

- **Sicherstellung der Optionalität des analogen Führscheins:** Es sollte sowohl aus verfassungsrechtlichen Gründen als auch im Kontext der

¹⁸ Auch resultiert hieraus in § 75 Nr. 4c FeV-E der Tatbestand einer Ordnungswidrigkeit.

¹⁹ S. hierzu *Schnermann*, „Digitaler Führerschein - Sicherheit braucht Schnittstellen, nicht Symbolpolitik“, TSPBackground Verkehr & Smart Mobility v. 10.10.2025, <https://background.tagesspiegel.de/verkehr-und-smart-mobility/briefing/sicherheit-braucht-schnittstellen-nicht-symbolpolitik> (abgerufen am 18.2.2025).

²⁰ Dieses enthält nach § 50 Abs. 1 Nr. 2 StVG sowie § 49 Abs. 1 Nr. 17 FeV auch Hinweise auf Eintragungen im Fahreignungsregister über bestehende Einschränkungen des Rechts, die Fahrerlaubnis zu gebrauchen.

datenschutzrechtlichen Einwilligung dauerhaft und ausdrücklich sichergestellt sein, dass der analoge Führerschein dem digitalen Führerschein in sämtlichen Kontroll-, Verwaltungs- und Nutzungskontexten praktisch gleichwertig bleibt und aus der Nichtnutzung der digitalen Variante keinerlei rechtliche oder faktische Nachteile entstehen.

- **Gewährleistung der Informiertheit der Einwilligung:** Die Einwilligung in den Abruf und die Verarbeitung des Lichtbildes zur Generierung des digitalen Führerscheins ist durch eine transparente, verständliche und barrierefreie Ausgestaltung des Antragsverfahrens so auszugestalten, dass Umfang, Zweck, Rechtsfolgen und Widerrufsmöglichkeiten der Verarbeitung für die Antragsteller klar und eindeutig erkennbar sind.
- **Hohe Relevanz der Gestaltung des technischen Standards im Hinblick auf Datenschutz, Datensicherheit und IT-Sicherheit:** Bei der Entwicklung des technischen Standards nach § 2d Abs. 3 StVG-E sind Datenschutz-durch-Technikgestaltung, strikte Datenminimierung, sichere Verschlüsselungs- und Authentifizierungsverfahren sowie eine vor allem mit Blick auf die EUid-Brieftasche interoperable Sicherheitsarchitektur verbindlich zu verankern.
- **Sicherstellung von Praxisgerechtigkeit und Aktualität:** Für einen effektiven und rechtskonformen Vollzug ist sicherzustellen, dass der digitale Führerschein offline nutzbar ist und zeitnah aktualisiert wird, sodass Sperren oder Entziehungen der Fahrerlaubnis zuverlässig und aktuell abgebildet werden.

D. Digitale Parkraumüberwachung

§ 63g StVG-E soll eine effektive Parkraumbewirtschaftung ermöglichen. Dieses Ziel ist begrüßenswert – die hierzu konkret vorgeschlagene Maßnahme bedarf unterdessen einer genaueren rechtlichen Betrachtung: Sowohl aus europarechtlicher als auch aus verfassungsrechtlicher Perspektive bedarf ein solches Vorhaben deshalb einer detaillierten Auseinandersetzung mit den einschlägigen Grundrechten, der Rechtsprechung des Bundesverfassungsgerichtes und europäischem Sekundärrecht. Ohne den Anspruch einer abschließenden Bewertung wird im Folgenden zunächst die relevante Rechtsprechung dargestellt, um dann besonders problematische Eckpunkte des Vorhabens hervorzuheben und Vorschläge für eine möglichst datensparsame Umsetzung zu unterbreiten.

I. Verfassungsrechtliche Maßstäbe

1. Anwendbare Grundrechtsordnung

Zwar sind mittlerweile weite Bereiche des Datenschutzrechts europarechtlichen Ursprungs, jedoch ist eine vollständige unionsrechtliche Determination des vorliegenden Bereichs nicht anzunehmen, sodass mit der Rechtsprechung des Bundesverfassungsgerichts²¹ weiterhin die nationalen Grundrechte angewandt werden können.²²

2. Grundrechtsrelevante Vorgänge

Ziel des Datenschutzes ist der Schutz der Privatsphäre und die Hoheit des Einzelnen über seine Daten.²³ Zentral ist dabei das Recht auf informationelle Selbstbestimmung, welches das Bundesverfassungsgericht in ständiger Rechtsprechung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ableitet.²⁴ Es gewährt dem Einzelnen das Recht „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“²⁵. **Kfz-Kennzeichen sind personenbezogene Daten**, da sie eine Identifizierbarkeit der betroffenen Personen ermöglichen.²⁶ Bei der Bewertung der Maßnahme muss die mögliche Erfassung von Passanten und fahrenden Kfz ebenso berücksichtigt werden. Vollständig anonymisierte Daten fallen hingegen nicht in den Schutzbereich des Rechts auf informationelle Selbstbestimmung.²⁷

Die Erhebungen, Speicherung, Verwendung und Weitergabe von personenbezogenen Daten stellen rechtfertigungsbedürftige Eingriffe in das Recht auf informationelle Selbstbestimmung dar.²⁸ Grundrechtsrelevant in § 63g StVG-E sind damit folgende Vorgänge:

- Die Schaffung der Möglichkeit für die zuständigen Behörden, Parkende zu einer **Eingabe des Kennzeichens zu verpflichten** (§ 63g Abs. 1 S. 1 StVG-E).
- Die **Speichererlaubnis** (§ 63g Abs. 1 S. 2 StVG-E) der Daten bis zu 24 Stunden nach Ende des Geltungszeitraums.

²¹ Sofern der nicht vollständig unionsrechtlich determinierte Bereich Raum für die Anwendung nationaler Grundrechte lässt, prüft das Bundesverfassungsgericht primär anhand der deutschen Grundrechte. Es berücksichtigt bei der Auslegung allerdings auch die Unionsgrundrechte. Liegt das Schutzniveau des Grundgesetzes unterhalb des Schutzniveaus der europäischen Grundrechtecharta, so ist die Grundrechtecharta Maßstab der Grundrechtsprüfung. BVerfGE 152, 216 Rn. 42 ff.

²² Vgl. zum Verhältnis von GRCh zum GG im Sicherheitsrecht *Lisken/Denninger*, in: PolR-HdB/Müller/Schwaabenbauer, 7. Aufl. 2021, G. Rn. 385 ff.

²³ *Heckmann/Paschke*, in: Stern/Sodan/Möstl StaatsR, 2. Aufl. 2022, § 103 Rn. 7.

²⁴ Vgl. BVerfGE 156, 11 Rn. 71; *Heckmann/Paschke*, in: Stern/Sodan/Möstl StaatsR, 2. Aufl. 2022, § 103 Rn. 9, jeweils m.w.N.

²⁵ Vgl. BVerfGE 156, 11 Rn. 71; *Heckmann/Paschke*, in: Stern/Sodan/Möstl, 2. Aufl. 2022, § 103 Rn. 11, jeweils m.w.N.

²⁶ BVerfGE 150, 244 Rn. 40.

²⁷ BVerfGE 65, 1, 45 ff.; *Heckmann/Paschke*, in: Stern/Sodan/Möstl, 2. Aufl. 2022, § 103 Rn. 11.

²⁸ *Di Fabio*, in: Dürig/Herzog/Scholz GG, 108. EL August 2025, Art. 2 Abs. 1 GG Rn. 176.

- Die **Erlaubnis** der zuständigen Behörden, diese Daten und die Daten der Kfz-Kennzeichen, Geltungsbereiche und Geltungszeiträume dauerhafter Parkberechtigungen zur Kontrolle der Parkberechtigung **zu verarbeiten** (§ 63g Abs. 1 S. 3 StVG-E).
- Die Datenerhebung durch **optisch-elektronische Einrichtungen** zum Zweck der Kontrolle der **Parkberechtigung** (§ 63g Abs. 2 S. 1 StVG-E).
- Die **Übermittlung** dieser Daten (§ 63g Abs. 2 S. 1 StVG-E).
- Deren **Speicherung** (§ 63g Abs. 2 S. 1 StVG-E).
- Der **automatisierte Abgleich** (§ 63g Abs. 2 S. 2 StVG-E) dieser Daten mit den Daten über die dauerhaften Parkberechtigungen (§ 63g Abs. 1 S. 3 StVG-E) und den Daten der kurzzeitigen Parkberechtigungen (§ 63g Abs. 1 S. 2 StVG-E).
- Die **Weiterverarbeitung** der Daten nach Überprüfung des Ergebnisses der fehlenden Parkberechtigung (mit oder ohne Sichtkontrolle) (§ 63g Abs. 2 S. 3, 5 StVG-E).
- Die **Datenerhebung und -verarbeitung** durch die Videokontrolle zur Überprüfung des **regelwidrigen Parkens/Haltens** unabhängig von der Parkberechtigung (§ 63g Abs. 3 S. 1 StVG-E).
- Die **automatisierte Weiterverarbeitung** der in § 63g Abs. 3 S. 2 StVG-E genannten Daten bei „hinreichend sicher[em]“ Verstoß (§ 63g Abs. 3 S. 2 StVG-E) bzw. bei Feststellung eines erneuten Verstoßes durch eine Videokontrolle oder eine Überwachungskraft (§ 63g Abs. 3 S. 4 StVG-E).
- Die **Speicherung, sofern sich nur Anhaltspunkte** für einen Verstoß ergeben haben, welche einer erneuten Kontrolle bedürfen (§ 63g Abs. 3 S. 3 StVG-E).

All diese Vorgänge sind mit rechtfertigungsbedürftigen Grundrechteingriffen verbunden. Aufgrund der Neuartigkeit dieser innovativen Form einer digitalen Parkraumüberwachung kann nicht mit abschließender Sicherheit beurteilt werden, inwiefern das Gesetzesvorhaben in einem Verfahren vor dem Bundesverfassungsgericht Bestand hätte. Da Teile der Maßnahme aber Ähnlichkeiten zu verschiedenen, bereits existierenden sicherheits- und verkehrsrechtlichen Maßnahmen aufweisen, lässt sich bei der verfassungsrechtlichen Bewertung auf vergangene Rechtsprechung zurückgreifen.

3. Besonders relevante Rechtsprechung

Insbesondere der Entscheidung des BVerfG zur KfZ-Kennzeichenerfassung,²⁹ der Entscheidung zu HessenDATA,³⁰ den Entscheidungen des BVerfG³¹ und BVerwG³² zur

²⁹ BVerfGE 150, 244.

³⁰ BVerfGE 165, 363.

³¹ BVerfG NVwZ 2007, 688.

³² BVerwG NVwZ 2012, 757.

Videoüberwachung öffentlicher Plätze und der Entscheidung des BVerfG zu Geschwindigkeits-, „Blitzern“³³ lassen sich Eckpunkte für eine Bewertung entnehmen.

a) Kfz-Kennzeichenkontrolle

Die in dem Verfahren im Jahr 2018 überprüfte Norm des BayPAG ermächtigte die Polizei dazu „bei entsprechenden Lageerkenntnissen“ in Fällen, welche nach dem bayerischen PAG auch eine Identitätsfeststellung ermöglichen würden, Kennzeichen von Kfz inklusive Ort, Datum, Uhrzeit und Fahrtrichtung zu erfassen und mit einem Fahndungsbestand abzugleichen.³⁴

Das Gericht entschied, dass bei allen erfassten Fahrzeugen ein **Eingriff in das Recht auf informationelle Selbstbestimmung** vorliege. In Abweichung zu vorausgegangener Rechtsprechung³⁵ ging das Gericht auch bei sog. Nichttreffern, welche nach dem Abgleich sofort gelöscht werden, von einem Eingriff aus, da durch die Kontrolle ein verdichtetes behördliches Interesse an ihnen bestünde und sie nicht nur technikbedingt miterfasst würden.³⁶ Im Gegensatz zu Geschwindigkeitskontrollen würden personenbezogene Daten nicht erst nach der Feststellung einer Übertretung erhoben.³⁷

Das Bundesverfassungsgericht hielt die Vorschrift des BayPAG für unvereinbar mit dem Verhältnismäßigkeitsgrundsatz. Auch wenn es das Fahndungsinteresse anerkannte, fehlte nach Ansicht des Gerichts ein hinreichender Anlass:

„Die Durchführung von Kontrollen zu beliebiger Zeit und an beliebigem Ort ins Blaue hinein ist mit dem Rechtsstaatsprinzip grundsätzlich unvereinbar.“³⁸

Dennoch seien **anlasslose Kontrollen** nicht grundsätzlich ausgeschlossen. Eine Zulässigkeit könne begründet werden, wenn der Grund solcher Kontrollen in **gefährlichen risikobehafteten Tätigkeiten oder Gefahrenquellen** liege und eine sich hieraus ergebende Gefahr adressiert werde. Dann entspreche die Situation zulässigen **stichprobenhaft durchgeführten Verkehrskontrollen**.³⁹

Unter anderem forderte das Gericht **Dokumentationspflichten**⁴⁰ und wertete im Rahmen der verfassungsrechtlichen Anforderungen die **unverzügliche Löschpflicht** nach Abgleich von Nichttreffern positiv. Das Gericht erläuterte, dass in der **Nutzung der Daten**

³³ BVerfG NJW 2010, 2717.

³⁴ BVerfGE 150, 244 Rn. 2ff.

³⁵ BVerfGE 120, 378.

³⁶ BVerfGE 150, 244 Rn. 48-51.

³⁷ BVerfGE 150, 244 Rn. 52.

³⁸ BVerfGE 150, 244 Rn. 92.

³⁹ BVerfGE 150, 244 Rn. 94.

⁴⁰ BVerfGE 150, 244 Rn. 153f.

zu anderen Zwecken ein weiterer Grundrechtseingriff liege, welcher seinerseits rechtfertigungsbedürftig sei.⁴¹ Das in der Norm enthaltene grundsätzliche **Verbot der Erstellung eines Bewegungsbildes** begrüßte das Gericht.⁴²

b) HessenDATA

In der Entscheidung HessenDATA ging es um eine Anwendung automatisierter Datenanalyse von Datenbeständen der Polizei. Dieses Urteil ist für die Bewertung der Parkraumüberwachung insoweit relevant, als das BVerfG darin zum Ausdruck bringt, dass die **Verwendung lernfähiger Systeme und komplexer deterministischer Systeme eingriffstiefend** wirken kann.⁴³ Dies begründet das Gericht unter anderem mit der Opazität der Systeme, welche die Nachvollziehbarkeit von Ergebnissen beeinträchtigen kann.⁴⁴

c) Videoüberwachung

Ergänzend ist noch auf die Entscheidung des BVerwG aus dem Jahr 2012 zu Videoüberwachung einzugehen. In dem Urteil kommt die Erforderlichkeit einer restriktiven Handhabung von Videoüberwachung seitens des Staates zum Ausdruck:

„Die anlasslose Überwachung des öffentlichen Straßenraums stellt einen erheblichen Grundrechtseingriff dar, insbesondere für Menschen, die aus persönlichen oder beruflichen Gründen gezwungen sind, sich dieser Beobachtung häufig auszusetzen“⁴⁵

Das Gericht hielt die örtlich begrenzte Videoüberwachung aufgrund der damit einhergehenden Schutzwirkung für betroffene Passanten, der Offenheit des Einsatzes, der Beschränkung der Beobachtung auf öffentliches Verhalten, des **Ausnahmecharakters** und der **wiederholt begangenen Straftaten im betroffenen Bereich** für zulässig.⁴⁶ Die Möglichkeit einer **Verpixelung bestimmter Bereiche**, welche für die Schutzzwecke nicht erforderlich sind, wird in dem Urteil als mögliche mildere Durchführung angedeutet.⁴⁷ Mit der Entscheidung verfolgt das BVerwG die Rechtsprechungslinie des BVerfG von 2007. Das Bundesverfassungsgericht hatte klargestellt, dass neben einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage eine Videoüberwachung öffentlicher Einrichtungen einen **hinreichenden Anlass** und eine **verhältnismäßige Begrenzung räumlicher und zeitlicher Art** bedürfe und die Möglichkeiten der **Datenauswertung** verhältnismäßig gestaltet sein müssten.⁴⁸

⁴¹ BVerfGE 150, 244 Rn. 153ff.

⁴² BVerfGE 150, 244 Rn. 166.

⁴³ BVerfGE 165, 363, Rn. 100.

⁴⁴ BVerfGE 165, 363, Rn. 100f.

⁴⁵ BVerwG NVwZ 2012, 757 Rn. 47.

⁴⁶ BVerwG NVwZ 2012, 757 Rn. 47f.

⁴⁷ BVerwG NVwZ 2012, 757 Rn. 53.

⁴⁸ BVerfG NVwZ 2007, 688.

d) Fotografische Erfassung von Geschwindigkeitsverstößen

Die Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2010 zur Zulässigkeit sog. „Blitzer“ verdeutlicht den Unterschied zwischen anlasslosen und **anlassbezogenen Eingriffen** in das Recht auf informationelle Selbstbestimmung. Das Gericht stellte klar, dass durch eine Bildaufnahme von Fahrer und Kennzeichen nur personenbezogene Daten von den Personen erhoben würden, welche durch die vom Messgerät festgestellte Geschwindigkeitsüberschreitung auch einen Anlass für den Eingriff gesetzt haben.⁴⁹ Andere Personen dürften nur bei Unvermeidbarkeit betroffen sein.⁵⁰ Außerdem seien **Einschüchterungseffekte** deshalb **nicht zu erwarten**, weil Ziel der Maßnahme **nur die Einhaltung der Geschwindigkeitsregelungen** sei und außer der Verfolgung dieser Verkehrsordnungswidrigkeiten keine belastenden Auswirkungen für Betroffene bestünden.⁵¹

II. Bewertungen und Empfehlungen

1. Eingabepflicht des Kfz-Kennzeichens, § 63g Abs. 1 StVG-E

Die verpflichtende Eingabe personenbezogener Daten stellt, wie in der Entwurfsbegründung dargelegt,⁵² einen **Eingriff** in das Recht auf informationelle Selbstbestimmung dar. Zwar ließe sich vertreten, dass in dem Parken eine eingriffsausschließende Einwilligung liegt, allerdings ist diese Argumentation mit Blick auf die Rechtsprechung zu Videoüberwachung öffentlicher Plätze⁵³ angreifbar.

Dementsprechend **wichtig und begrüßenswert** sind deshalb **das Verbot der Verarbeitung der Daten für andere Zwecke, das Verbot der Beschlagnahme der Daten** nach anderen Rechtsvorschriften und **das Verbot der Verarbeitung zur Erstellung eines Profils** (§ 63g Abs. 6 StVG-E), aber auch die **Begrenzung der Speicherdauer** (§ 63g Abs. 1 S. 1 StVG-E).

Die in § 63g Abs. 1 StVG-E vorgesehene Umwandlung des Kfz-Kennzeichens in einen **Hash-Wert führt nicht zwangsläufig zu einer Anonymisierung**,⁵⁴ welche den

⁴⁹ BVerfG NJW 2010, 2717 Rn. 14.

⁵⁰ BVerfG NJW 2010, 2717 Rn. 14.

⁵¹ BVerfG NJW 2010, 2717 Rn. 14.

⁵² BT-Drs. 21/3505 S. 43.

⁵³ Vgl. zu Videoüberwachung BVerfG NVwZ 2007, 688.

⁵⁴ S. Kuß, in: Hornung/Schallbruch IT-Sicherheitsrecht, 2. Aufl. 2024, § 28 Rn. 80f; Klar/Kühling, in: Kühling/Buchner, DSGVO BDSG, 4. Auflage 2024, Art. 4 Nr. 1 DSGVO Rn. 34; vgl. auch Schwartmann/Jaspers/Lep-perhoff/Weiß/Meier, Praxisleitfaden zum Anonymisieren personenbezogener Daten, 02.12.2022, abrufbar unter: https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/Anonymisierung_personenbezogener_Daten/SDS_Studie_Praxisleitfaden-Anonymisieren-Web_01.pdf (zuletzt abgerufen am 02.02.2026), S. 36f.; als mögliche Anonymisierungsmethode aufgeführt, allerdings mit dem Hinweis, dass das Verfahren keinen automatischer Schutz vor Entschlüsselung bietet: Bundesverband der Deutschen Industrie e.V., Anonymisierung personenbezogener Daten, Stand Oktober 2020, abrufbar unter: [*20201103 Leitfaden BDI Anonymisierung personenbezogener Daten.pdf](https://www.bdi-online.de/fileadmin/user_upload/20201103_Leitfaden_BDI_Anonymisierung_personenbezogener_Daten.pdf) (zuletzt abgerufen am: 02.02.2026), S. 21; allgemeine Erläuterung zu Hash-Werten: Frey, GRUR-Prax 2024, 60.

Personenbezug von Daten aufheben würde. Ob in dem Entwurf von einer solchen Anonymisierung ausgegangen wird oder durch die Umwandlung in Hashwerte lediglich ein Schutzinstrument vor Datenmissbrauch gesehen wird, ist nicht ersichtlich.⁵⁵ Der Entwurf geht davon aus, dass durch die Umwandlung der Kfz-Kennzeichen in Hashwerte eine Ermittlung des Kennzeichens nur mit unverhältnismäßigem Aufwand möglich ist.⁵⁶ Nach Rechtsprechung des EuGH kann ein solcher unverhältnismäßiger Aufwand eine Aufhebung des Personenbezugs der Daten bewirken.⁵⁷ Es ist davon auszugehen, dass die Behörde den Algorithmus, welcher zur Umwandlung in einen Hash-Wert verwendet wird, kennt. Die Kenntnis des Algorithmus könnte als Zusatzwissen zu werten sein, welches es ermöglicht, den Personenbezug der Daten wieder herzustellen.⁵⁸ Außerdem wird durch die durchgeführten Videokontrollen der Personenbezug bei Parkberechtigung im Abgleichvorgang wieder hergestellt. Aus diesem Grund wird eine genauere Auseinandersetzung mit dem Verfahren zur Erzeugung des Hash-Werts und deren Auswirkungen auf den Personenbezug der Daten empfohlen.

Um die Risiken von Missbrauch zu minimieren, ist außerdem die Einhaltung von **IT-Sicherheitsstandards** bedeutsam.

2. Mobile optisch-elektronische Einrichtungen (Videokontrollen), § 63g Abs. 2 und 3 StVG-E

Wie bereits dargestellt, sind die Videokontrollen mit Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden. Dabei kann zwischen den Eingriffen in die Rechte der Parkenden und Eingriffen in die durch die Kontrolle miterfassten Personen, wie etwa Passanten und fahrende Kfz, unterschieden werden.

Eine Einwilligung der betroffenen Person in die Datenerhebung kann einen Eingriff in das Recht auf informationelle Selbstbestimmung entfallen lassen.⁵⁹ Die **Annahme einer eingriffsausschließen Grundrechtsausübung oder Einwilligung** in die Datenerhebung ist aufgrund der Argumentation des Bundesverfassungsgerichts, welches eine solche bei Videoüberwachung öffentlicher Einrichtungen ablehnte,⁶⁰ aber **problematisch**, da sich viele Menschen im öffentlichen Raum mit dem Kfz fortbewegen und damit auch das Bedürfnis einhergeht, an bestimmten Orten zu parken, um bspw. zur Arbeit zu gehen, einzukaufen oder schlicht am öffentlichen Leben teilzunehmen. Diese Argumentation gilt auch für die Erfassung personenbezogener Daten Dritter, auf welche sich kein Kontrollinteresse erstreckt.

⁵⁵ Offengelassen, ob durch die Speicherung als Hash-Wert eine Pseudonymisierung oder Anonymisierung anzunehmen ist: BT-Drs. 21/3505, S. 45.

⁵⁶ BT-Drs. 21/3505, S. 44.

⁵⁷ EuGH NJW 2025, 3415 Rn. 82.

⁵⁸ Vgl. dazu Kuß, in: Hornung/Schallbruch IT-Sicherheitsrecht, 2. Aufl. 2024, § 28 Rn. 80.

⁵⁹ Heckmann/Paschke, in: Stern/Sodan/Möstl StaatsR, § 103 Rn. 48f.

⁶⁰ BVerfG NVwZ 2007, 688, 690.

Die Möglichkeit einer **verfassungsrechtlichen Rechtfertigung** des Eingriffs bestimmt sich nach der Verhältnismäßigkeit. Legitimes Ziel, Geeignetheit und Erforderlichkeit dürfen, legt man die Annahme einer Kostensenkung und Effektivitätssteigerung zu Grunde, bei den Maßnahmen nach § 63g Abs. 2 und Abs. 3 StVG-E zu bejahen sein. In der dann vorzunehmenden Abwägung im Rahmen der Verhältnismäßigkeit ist der Eingriffstiefe das Gewicht des bezweckten Ziels gegenüberzustellen.

Das bezweckte **Ziel der effektiven Parkraumbewirtschaftung** ist überaus relevant und begrüßenswert. Jedoch weist es über die erwartete Verringerung der Parksuchverkehrs und von behinderndem oder gefährdendem Falschparken nur mittelbaren Bezug zu Gütern wie Leib, Leben oder bedeutende Sachwerte auf.⁶¹

Bei der **Bewertung des Eingriffsgewichts** ist eingriffsmindernd zu berücksichtigen, dass nur Daten aus Aktivitäten im öffentlichen Raum erhoben werden, die Kfz-Kennzeichen nur mittelbar einen Personenbezug aufweisen, bei der Feststellung des berechtigten (§ 63g Abs. 2 StVG-E) und regelkonformen (§ 63g Abs. 3 StVG-E) Parkens keine unmittelbaren Folgen zu erwarten sind und es sich um eine offen erfolgende Maßnahme handelt.⁶² Auch die Speicherung als Hashwert könnte sich eingriffsmindernd auswirken. Demgegenüber wirkt eingriffserhöhend, dass eine unbestimmte Vielzahl an Personen betroffen ist, die selbst keinerlei Anlass gesetzt haben.⁶³ Im Gegensatz zu Geschwindigkeitsmessungen und anschließendem Blitzen⁶⁴ stellt die Parkraumüberwachung einen anlasslosen Eingriff dar, da bereits unabhängig von einem regelwidrigen Verhalten personenbezogene Daten erhoben werden.

Inwiefern die Maßnahmen tatsächlich in einem Verfahren vor dem Bundesverfassungsgericht als verhältnismäßig bewertet würden, kann hier nicht abschließend geklärt werden und bleibt einer Entscheidung des Gerichts vorbehalten.

In dem Entwurf wurden bereits wichtige Aspekte für eine grundrechtsschonende Ausgestaltung erkannt und normiert. Diese sollten beibehalten werden. Im Folgenden wird außerdem aufgezeigt, wie das Eingriffsgewicht weiter gesenkt werden könnte, um eine möglichst grundrechtsschonende und damit auch verfassungskonforme Durchführung der Maßnahme sicherzustellen.

⁶¹ Der Entwurf geht davon aus, dass das Gesetz deshalb auch dem Schutz von Rechtsgütern mit erheblichem Gewicht dient, namentlich dem Schutz der Gesundheit, des Lebens und bedeutender Sachwerte, aber auch der Leichtigkeit des Verkehrs und der Vermeidung von schädlichen Umwelteinflüssen, BT-Drs. 21/3505, S. 44.

⁶² Vgl. BVerfGE 150, 244 Rn. 97.

⁶³ Vgl. BVerfGE 150, 244 Rn. 98.

⁶⁴ BVerfG NJW 2010, 2717 Rn. 14.

a) Anlasslosigkeit und Streubreite der Maßnahmen

Die Anlasslosigkeit und Streubreite einer Maßnahme führt zu einer gesteigerten Eingriffsintensität und damit zu höheren Anforderungen an die Eingriffsrechtfertigung.

Wie bereits ausgeführt, stellte das Bundesverfassungsgericht in dem Urteil zur Kfz-Kennzeichenerfassung dar, dass auch anlasslose Kontrollen möglich seien, sofern diese an gefährliches Verhalten anknüpfen. Als Beispiel führt das Gericht stichprobenartig ausgeführte Verkehrskontrollen an. Insofern lässt sich vertreten, dass eine digitale Parkraumüberwachung verfassungskonform sein kann, wenn sie den **Charakter einer Stichprobe** wahrt. Dass dieses Erfordernis sowohl in § 63g Abs. 2 StVG-E als auch § 63g Abs. 3 StVG-E normiert wurde, ist begrüßenswert und sollte nach Ansicht der Verfasser entgegen des Antrags des Bundesrates⁶⁵ beibehalten werden.

Sowohl die Parkraumüberwachung nach § 63g Abs. 2 StVG-E als auch die Kontrolle nach § 63g Abs. 3 StVG-E weisen eine hohe Streubreite auf, selbst wenn, wie im Folgenden noch ausgeführt wird, ein Eingriff in Grundrechte von Passanten und fahrenden Kfz ausgeschlossen würde und nur bei parkenden Kfz von einem Eingriff in das Recht auf informationelle Selbstbestimmung ausgegangen wird. Da sich die nach § 63g Abs. 2 StVG-E ermöglichte Kontrolle auf bewirtschafteten Parkraum bezieht, ist die Streubreite geringer als bei Maßnahmen nach § 63g Abs. 3 StVG-E. Mangels Einschränkung im Gesetzestext wäre eine Überprüfung des gesamten Gebiets der betroffenen Gemeinde denkbar. Um die Eingriffsintensität zu verringern, könnte der Gesetzgeber über eine **Einschränkung der Maßnahme auf gefährdete Gebiete**⁶⁶ nachdenken, also die Kontrolle auf solche Straßen beschränken, in welchen in der Vergangenheit wiederholt Parkverstöße festzustellen waren.

b) Möglichst geringe Datenerfassung

Für eine möglichst grundrechtsschonende Gestaltung des Verfahrens sollten nicht benötigte personenbezogene Daten nicht erfasst werden. Dies trägt zum einen dem Datenminimierungsgrundsatz Rechnung, zum anderen kann bei richtiger Ausgestaltung ein Eingriff in das Recht auf informationelle Selbstbestimmung sogar verhindert werden.

Insoweit positiv zu werten ist das Erfordernis, auf Aufnahmen erkennbare weitere personenbezogene Daten, insbesondere von Personen und Kfz-Kennzeichen, nach dem „**Stand der Technik**“ „**unkennlich**“ zu machen (§ 63g Abs. 2 S. 1 Nr. 1 und Abs. 3 S. 2 Nr. 1 StVG-E). Um die Anzahl derer, in deren Recht auf informationelle Selbstbestimmung eingegriffen wird, möglichst gering zu halten, ist allerdings eine **irreversible** Unkenntlichmachung

⁶⁵ S. BT-DS 21/3505, S. 57.

⁶⁶ Analog zu einer Videoüberwachung gefährdeter Gebiete s. BVerwG NVwZ 2012, 757 Rn. 48.

erforderlich. Nur diese verhindert einen Personenbezug der Daten.⁶⁷ In Anwendung der Rechtsprechung des BVerfG zu der Kfz-Kennzeichenkontrolle könnten die personenbezogenen Daten dann als „nur technikbedingt (...) miterfasst, aber unmittelbar nach der Erfassung technisch wieder anonym, spurenlos und ohne Erkenntnisinteresse (...) aussondert“ bewertet werden.⁶⁸ Eine irreversible Unkenntlichmachung hätte damit zur Folge, dass ein Eingriff in das Recht auf informationelle Selbstbestimmung der betreffenden Personen durch den jeweiligen Vorgang verneint werden könnte. Insoweit eine solche **irreversible Unkenntlichmachung technisch möglich** ist, sollte sie aufgrund der Grundrechtsrelevanz auch Eingang **in den Gesetzestext** finden.

Vor Implementierung einer Unkenntlichmachung sollte allerdings durch die Einstellung des Winkels der optisch-elektronischen Einrichtung eine **Erfassung von Personen allgemein verhindert werden** und eine **diesbezügliche Anforderung in den Gesetzestext** aufgenommen werden. Nachdem der Winkel darüber bestimmt, ob Dritte einen Grundrechtseingriff erleiden, handelt es sich um einen verfassungsrechtlich als wesentlich zu bewertenden Aspekt, welcher einer Normierung bedarf.

c) Automatische Datenverarbeitung

Der Einsatz komplexer deterministischer Algorithmen sowie die Verwendung Künstlicher Intelligenz bei der Datenauswertung können das Eingriffsgewicht vertiefen.⁶⁹ Vorliegend soll jedoch keine komplexe polizeiliche Datenanalyse ermöglicht werden. Dementsprechend geringer erscheinen sich hieraus ergebende Risiken, weshalb eine Anwendung der verfassungsgerichtlichen Rechtsprechung auf das Gesetzesvorhaben nicht zwingend ist.

Dennoch empfiehlt sich eine Auseinandersetzung mit den möglichen Systemen, mittels welcher die digitale Parkraumüberwachung umgesetzt werden soll. Besonders bei Systemen zur Erkennung von Falschparkern erscheint der Einsatz Künstlicher Intelligenz aus unserer Perspektive nicht abwegig.

Bedeutsam für die Bewertung des Einsatzes ist die **„false positive“ Rate**. Die „false positive“ Rate entscheidet darüber, wie viele regelkonforme Parker Grundrechtseingriffen durch die Anfertigung von Bildern, Speicherung und Weiterverarbeitung der Daten ausgesetzt sind. Insbesondere für die Bewertung der Verhältnismäßigkeit eines Einsatzes solcher Systeme ohne Kontrollpersonen (§ 63g Abs. 2 S. 5 StVG-E) sind Angaben zur Verlässlichkeit von Systemen der digitalen Parkraumüberwachung essenziell.

⁶⁷ DSK, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, abrufbar unter: https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf (zuletzt abgerufen am: 03.02.2026), S. 5.

⁶⁸ BVerfGE 150, 244 Rn. 43.

⁶⁹ BVerfGE 165, 363, Rn. 100f.

An dieser Stelle sei auch darauf verwiesen, dass bei der Kfz-Kennzeichenerfassung nach dem Abgleich im System eine visuelle Überprüfung durch den bedienenden Polizeibeamten stattfindet.⁷⁰ Insofern könnte der ermöglichte **Verzicht auf die Sichtkontrolle kritisch** sein (§ 63g Abs. 2 S. 5 StVG-E).⁷¹

d) Einschüchterungseffekte

Einschüchterungseffekte beschreiben eine Form der Selbstzensur aufgrund befürchteter negativer Konsequenzen wegen der Überwachung.⁷² Das nicht unumstrittene Kriterium⁷³ führt nach Rechtsprechung des Bundesverfassungsgerichts zu einer Vertiefung des Grundrechtseingriffs. Dadurch erhöhen sich die Rechtfertigungsanforderungen und gegebenenfalls kann sich daraus die Unverhältnismäßigkeit einer Maßnahme ergeben. In der Literatur wird angenommen, dass die Möglichkeit einer automatisierten Beobachtung zu einem Anpassungsdruck aus Angst vor möglichen negativen Konsequenzen führen kann, welcher die Grundrechtsausübung unterbindet oder einschränkt.⁷⁴ Beispielsweise wird für den Einsatz von Polizeirobotern angenommen, dass die Möglichkeit der Datenauswertung eine Einschüchterung bewirken kann.⁷⁵ Erschwerend könne die Mobilität des Roboters und die Unmöglichkeit der Antizipation, welche Orte erfasst werden, hinzukommen.⁷⁶ Diese Überlegungen lassen sich auf die mobile Videokontrolle zur Parkraumüberwachung übertragen. Entsprechend bedeutsam ist das **Verbot der Beschlagnahme** der Daten und das **Verbot der Verarbeitung** der Daten für andere Zwecke (§ 63g Abs. 6 StVG-E). Diese Schlussfolgerung wird durch das Urteil des Bundesverfassungsgerichts zu „Geschwindigkeitsblitzern“ unterstrichen. Das Gericht schloss einen Einschüchterungseffekt aus, da die Maßnahme nur auf die Durchsetzung von Geschwindigkeitsregelungen abziele und die Betroffenen außer der Verfolgung entsprechender Ordnungswidrigkeiten nichts zu befürchten hätten.⁷⁷ Darum lehnen wir die vom Bundesrat vorgeschlagene⁷⁸ erweiterte Nutzungsmöglichkeit der Daten ab. Im Kontext etwaiger Einschüchterungseffekte sind deshalb auch die vorgenommenen Restriktionen in § 63g Abs. 6 StVG-E positiv hervorzuheben. Durch den Ausschluss einer Verarbeitung der Daten für andere Zwecke, das Verbot

⁷⁰ BVerfGE 150, 244 Rn. 7; *Annussek*, Automatisierte Kraftfahrzeugkennzeichenüberprüfung in den Ländern, Duncker & Humblot 2018, S. 43 m.w.N.

⁷¹ Der Entwurf stellt zwar klar (BT-Drs. 21/3505, S. 44), dass in der Sachbearbeitung eine menschliche Überprüfung zu erfolgen habe, nichtsdestotrotz erfolgen bereits zuvor Grundrechtseingriffe durch die Speicherung zur Weiterverarbeitung (§ 63g Abs. 2 S. 3 StVG-E).

⁷² Vgl. z.B. BVerfG NVwZ 2007, 688, 690; *Staben*, Der Abschreckungseffekt auf die Grundrechtsausübung, Mohr Siebeck 2016.

⁷³ Kritisch z.B. *Barczak*, in: Dreier GG, 4. Aufl. 2023, GG Art. 2 Abs. 1 Rn. 101.

⁷⁴ *Kunze*, in: Chibanguza/Kuß/Steege KI-Hdb, 2. Aufl. 2022, 2. Teil: § 9 A. Rn. 103.

⁷⁵ *Kemper*, Der Polizeiroboter: Freund, Helfer, Datensammler, DSRITB 2024, 231, 233f.

⁷⁶ *Kemper*, Der Polizeiroboter: Freund, Helfer, Datensammler, DSRITB 2024, 231, 234.

⁷⁷ BVerfG NJW 2010, 2717 Rn. 14.

⁷⁸ Vorschlag der Erlaubnis die protokollierten Daten für Strafverfahren zu verwenden und eine Verwendung der Daten nach Abs. 1-4 für begrenzte Zwecke der Strafverfolgung und Gefahrenabwehr und Anregung des Bundestages die Möglichkeiten eines automatisierten Abgleichs mit dem polizeilichen Fahndungsdatenbestand zu prüfen. BT-Drs. 21/3505, S. 59f.

der Profilbildung oder der Beschlagnahme der Daten, werden **Missbrauchsrisiken** und **Einschüchterungseffekte minimiert**.

Im Gegensatz zu Blitzern, welche nur bei Überschreitung von Geschwindigkeiten eine Aufnahme auslösen, könnten Videokontrollen zur Parkraumüberwachung durchaus auch von Passanten als einschüchternd wahrgenommen werden. Um entsprechende Einschüchterungseffekte im Rahmen der **Ausübung des Versammlungsrechts gemäß Art. 8 GG** auszuschließen, könnte man einen entsprechenden Ausschluss der Durchführung von Videokontrollen im Vor- und Nachfeld sowie während einer grundrechtlich geschützten Versammlung im betroffenen Gebiet und dessen näheren Umkreis aufnehmen.

III. Sekundärrechtliche Vorgaben des Unionsrechts

Zutreffend fordert der Bundesrat⁷⁹ die Prüfung von KI-VO und JI-RL.

Sofern die entsprechenden Systeme zur Videokontrolle Künstliche Intelligenz im Sinne der KI-VO enthalten (insb. § 63g Abs.3 StVG-E), ist der Anwendungsbereich der KI-VO eröffnet. Fraglich ist, ob sich hieraus weitergehende Anforderungen ergeben, da, sofern die Systeme nicht als Hochrisiko-KI bewertet werden, nur allgemeine Transparenzanforderungen in Frage kämen. Es wird eine tiefergehende Prüfung empfohlen.

Neben der KI-VO weiterhin anwendbar⁸⁰ und im vorliegenden Szenario einschlägig ist zudem die JI-RL. Gemäß Art. 1 Abs. 1 JI-RL gilt sie u.a. bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten. Der Begriff der Straftat ist nach EG 13 JI-RL unionsrechtsautonom auszulegen. Erfasst kann dabei auch die Verhütung, Verfolgung und Ahndung von Ordnungswidrigkeiten sein.⁸¹ Geht man von der Anwendbarkeit der JI-RL aus, so ergäben sich hieraus bestimmte Anforderungen, welche beachtet werden müssten: Wir empfehlen eine eingehende Prüfung der Anwendbarkeit der Richtlinie, möglicherweise einschlägiger Normen und verweisen insbesondere auf Art. 11 JI-RL. Dieser **verbietet die ausschließlich auf einer automatisierten Verarbeitung beruhende Entscheidung mit negativen Rechtsfolgen** und erlaubt eine Ausnahme hiervon nur unter bestimmten Bedingungen. Auf Seite 44 des Gesetzesentwurfs wird klargestellt, dass Bußgeldbescheide nur nach vorheriger Prüfung durch einen Sachbearbeiter erlassen werden.⁸² Aus Klarstellungsgründen empfehlen wir, die **Aufnahme eines solchen Prüfungsvorbehalts** in den Gesetzestext für auf Grundlage der Videokontrollen festgestellte Verstöße zu prüfen. Ebenso sei auf die möglicherweise einschlägige Pflicht zur Durchführung

⁷⁹ BT-Drs. 21/3505, S. S. 57f.

⁸⁰ Art. 2 Abs. 7 KI-VO.

⁸¹ VG Regensburg, BeckRS 2019, 14915 Rn. 23ff.; Roggenkamp, in: Specht/Mantz DatenschutzR-HdB, 1. Aufl. 2019, § 21 Rn. 5-10.

⁸² BT-Drs. 21/3505, S. 44.

einer **Datenschutzfolgenabschätzung** nach Art. 27 JI-RL bzw. bei hohen Risiken für die Rechte und Freiheiten natürlicher Personen hingewiesen.

IV. Abschließende Handlungsempfehlungen

Wir begrüßen die beabsichtigte Effizienzsteigerung und Digitalisierung durch eine Einführung der digitalen Parkraumüberwachung, sehen jedoch einige verfassungsrechtliche Hürden bei der Umsetzung. Insbesondere empfehlen wir:

- **Beibehaltung der in § 63g Abs. 6 S. 1 StVG-E normierten Verbote der Verarbeitung der Daten für andere Zwecke, der Profilbildung und der Beschlagnahme der erhobenen Daten:** Diese Aspekte sind zentral für eine verfassungskonforme Ausgestaltung der digitalen Parkraumüberwachung. Sie dienen der Senkung des Eingriffsgewichts, dem Vorbeugen eines Datenmissbrauchs und der Verhinderung eines Einschüchterungseffektes.
- **Prüfung der Auswirkungen der Umwandlung der Kfz-Kennzeichen in Hashwerte auf den Personenbezug der Daten:** Sofern die Entwurfsverfasser der Annahme sind, dass die Umwandlung der Kfz-Kennzeichen in einen Hashwert eine Anonymisierung der Daten für die zuständigen Behörden bewirkt, empfehlen wir eine tiefergreifende Prüfung.
- **Beibehaltung des „stichprobenartigen“ Charakters der Videokontrollen nach § 63g Abs. 2 und 3 StVG-E:** Dieses Kriterium ist aufgrund der Anlasslosigkeit und Streubreite der Maßnahmen essenziell für die Verfassungskonformität der Maßnahmen.
- **Prüfung einer Einschränkung der von der Videokontrolle nach § 63g Abs. 3 StVG-E erfassten Gebiete auf „gefährdete Gebiete“:** Je nach angenommener Vergleichbarkeit der Maßnahme mit der verfassungsrechtlichen Zulässigkeit statischer Videoüberwachung zur Gefahrenabwehr könnte die Einschränkung für die Verfassungskonformität als notwendig zu erachten sein. Dabei ist zu berücksichtigen, dass diese Einschränkung den Nutzen der Videokontrollen schmälert.
- **Aufnahme der Bedingung der irreversiblen Unkenntlichmachung nach dem Stand der Technik (§ 63g Abs. 2 S. 1 Nr. 1 und Abs. 3 S. 2 Nr. 1 StVG-E):** Nur durch die Irreversibilität der Unkenntlichmachung nach dem Stand der Technik wird vermieden, dass unbeteiligte Passanten und Kfz von der Maßnahme in grundrechtsrelevanter Weise berührt werden.
- **Prüfung der Möglichkeit, durch die Wahl des Aufnahmewinkels der Kameras die Erfassung personenbezogener Daten zu minimieren und Aufnahme**

dieser Einschränkung in den Gesetzestext: Durch eine solche Einschränkung würde die Erfassung nicht benötigter personenbezogener Daten bereits auf Ebene der Datenerhebung auf ein Minimum beschränkt und damit das Eingriffsgewicht der Maßnahme insgesamt gesenkt.

- **Ermittlung der „false positive“ Rate von den einsatzfähigen Systemen:** Die „false positive“ Rate ist essenziell, um den Effizienzgewinn durch die Videokontrolle und damit deren Geeignetheit zur Erreichung des Ziels des Gesetzesentwurfs bewerten zu können. Zudem hängen die Eingriffsintensität der Maßnahme und damit die Anforderungen an deren verfassungsrechtliche Rechtfertigung auch davon ab, wie viele regelkonforme Parker systemseitig als regelwidrig bzw. unberechtigte Parker eingestuft werden und deren Daten daher gespeichert und ggf. weiterverarbeitet werden.
- **Prüfung der Verfassungskonformität des Verzichts auf die Sichtkontrolle (§ 63g Abs. 2 S. 5 StVG):** Durch den Verzicht auf eine Sichtkontrolle kommt es bei Systemfehlern möglicherweise zu Grundrechtseingriffen für regelkonforme Parker durch die Weiterverarbeitung der gespeicherten Daten zu Zwecken der Verfolgung der vermeintlichen Verkehrsordnungswidrigkeiten. Bei der Bewertung sollte die „false positive“ Rate des Systems berücksichtigt werden.
- **Prüfung und gegebenenfalls die Streichung der Speichermöglichkeit bei Anhaltspunkten in § 63g Abs. 3 S. 3 StVG-E:** Sollten systemseitig Erfassungs- und Verarbeitungsvorgänge dazu führen, dass das System nur Anhaltspunkte für einen Verstoß feststellen kann, erschwert dies die Rechtfertigung des mit der Speicherung der Daten verbundenen Grundrechtseingriffs. Hierbei ist auch relevant, inwiefern die Speicherung der Hashwerte der Kfz-Kennzeichen als Speicherung personenbezogener Daten gilt.
- **Aufnahme des Ausschlusses der Durchführung von Videokontrollen im Vor- und Nachfeld sowie während einer grundrechtlich geschützten Versammlung im betroffenen Gebiet und dessen näheren Umkreis:** Aus den Videokontrollen resultierende Einschüchterungseffekte könnten andernfalls dazu führen, dass Personen sich in der Ausübung der Versammlungsfreiheit einschränken.
- **Prüfung des Einsatzes von Künstlicher Intelligenz in den Systemen zur Videokontrolle und der damit einhergehenden Pflichten aus der KI-VO.**
- **Prüfung der Anwendbarkeit der JI-RL und ihrer Anforderungen,** insbesondere der Aufnahme eines Prüfvorbehalts durch Sachbearbeiter vor Ausstellung des Bußgeldbescheids durch die zuständige Behörde in den Gesetzestext.

E. Die Gutachterinnen und Gutachter

Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Recht und Sicherheit der Digitalisierung an der Technischen Universität München (TUM) sowie Direktor des TUM Center for Digital Public Services (TUM CDPS). Außerdem ist er Mitglied des Direktoriums des Bayerischen Forschungsinstituts für Digitale Transformation (bidt) sowie seit 2003 nebenamtlicher Verfassungsrichter am Bayerischen Verfassungsgerichtshof. Er forscht, lehrt und berät seit mittlerweile fast 30 Jahren im Schnittfeld von Recht, IT, Politik und Verwaltung. In diesem Rahmen war er u.a. Mitglied der Ethikkommission des Bundesverkehrsministeriums zum Automatisierten und Vernetzten Fahren.

Ass. iur. Joanna Klauser ist seit 2024 wissenschaftliche Referentin am bidt (Bayerisches Forschungsinstitut für digitale Transformation) und Doktorandin bei Prof. Dr. Dirk Heckmann. Ihre Forschungsschwerpunkte liegen im Verfassungs-, Sicherheits- und Strafprozessrecht.

Ass. iur. Pascal Bronner ist seit 2022 Doktorand und wissenschaftlicher Mitarbeiter am Lehrstuhl für Recht und Sicherheit der Digitalisierung bei Prof. Dr. Dirk Heckmann. Seine Forschungsschwerpunkte liegen im Daten- und Datenschutzrecht sowie dem Recht der Künstlichen Intelligenz.