# Recht der Digitalisierung II

Herausgegeben von
PHILIPP ANZENBERGER
und KLAUS SCHWAIGHOFER

*Internet und Gesellschaft*
*41*

**Mohr Siebeck**

Internet und Gesellschaft

Schriften des Alexander von Humboldt Institut
für Internet und Gesellschaft

Herausgegeben von

Jeanette Hofmann, Matthias C. Kettemann,
Björn Scheuermann, Thomas Schildhauer
und Wolfgang Schulz

41

# Recht der Digitalisierung II

## Internationalisierung der Justiz im digitalen Zeitalter

Herausgegeben von
Philipp Anzenberger und Klaus Schwaighofer

Mohr Siebeck

*Philipp Anzenberger*, geboren 1986, Studium der Rechtswissenschaften, sowie der Betriebswirtschaftslehre und Geographie (im Rahmen von Umweltsystemwissenschaften), 2014 Promotion zum Doktor der Rechtswissenschaften, 2019 Habilitation für die Fächer Zivilverfahrensrecht und Bürgerliches Recht, seit 2022 Universitätsprofessor am Institut für Zivilgerichtliches Verfahren der Leopold-Franzens-Universität Innsbruck.

*Klaus Schwaighofer*, geboren 1956, 1979 Promotion zum Doktor der Rechte, 1987 Habilitation für das Fach Strafrecht, Strafprozessrecht und Kriminologie, 1996 Ernennung zum Universitätsprofessor für Strafrecht, Strafprozessrecht und Kriminologie an der Leopold-Franzens-Universität Innsbruck, seit 1.10.2024 emeritiert.

ISBN 978-3-16-162589-3 / eISBN 978-3-16-162590-9
DOI 10.1628/978-3-16-162590-9

ISSN 2199-0344 / eISSN 2569-4081 (Internet und Gesellschaft)

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind über *https://dnb.dnb.de* abrufbar.

Publiziert von Mohr Siebeck Tübingen 2025.



Gedruckt auf alterungsbeständiges Papier. Satz: Laupp & Göbel, Gomaringen.

Mohr Siebeck GmbH & Co. KG, Wilhelmstraße 18, 72074 Tübingen, Deutschland
www.mohrsiebeck.com, info@mohrsiebeck.com

# Vorwort der Herausgeber

Die Leopold-Franzens-Universität Innsbruck hat vor einigen Jahren beschlossen, einen Forschungsschwerpunkt im Bereich der Digitalisierung und Internationalisierung zu setzen. Zur Umsetzung dieses Schwerpunkts veranstaltet die Rechtswissenschaftliche Fakultät seit Sommersemester 2023 eine Ringvorlesung zu diesen Themen, wobei alternierend verschiedene Institute federführend sind. Zum Auftakt fand im März 2023 der vom Institut für Theorie und Zukunft des Rechts organisierte erste Digitalrechtstag statt. Die Vorträge auf dieser Tagung wurden im ersten Band „Recht der Digitalisierung: Herausforderungen der digitalen Governance in Wendezeiten" veröffentlicht.

Der nun vorliegende zweite Band enthält die Schriftfassungen aller Vorträge, die im Rahmen der Ringvorlesung im Wintersemester 2023/24 und im Sommersemester 2024 an der Universität Innsbruck gehalten wurden: Die Vorträge im Wintersemester 2023/24 wurden vom Institut für Strafrecht, Strafprozessrecht und Kriminologie organisiert und behandeln verschiedene Aspekte der Digitalisierung und Internationalisierung im Bereich des materiellen Strafrechts und Strafverfahrensrechts: *Severin Glaser* beschäftigt sich mit strafbaren Handlungen mit Kryptowährungen und unbaren Zahlungsmitteln, *Lorenzo Picotti* mit Künstlicher Intelligenz und Strafrecht, *Klaus Schwaighofer* mit dem Einsatz der Videotechnologie im Strafverfahren und deren Vereinbarkeit mit den Prozessgrundsätzen, *Andreas Venier* mit der Sicherstellung und Auswertung von Daten (insb. Smartphones), *Konrad Kmetic* mit dem Beitrag der Europäischen Staatsanwaltschaft zur grenzüberschreitenden Strafverfolgung und *Günther Hauss* mit der Europäischen Bankenaufsicht und Sanktionen gegen systemrelevante Banken in Europa.

Die Vorträge im Sommersemester 2024 waren thematisch der Digitalisierung und Internationalisierung im Zivil- und Zivilverfahrensrecht gewidmet und wurden vom den Instituten für Zivilrecht, Zivilgerichtliches Verfahren und Unternehmensrecht organisiert. Der Beitrag von *Philipp Anzenberger* beschäftigt sich mit Videoverhandlungen und Videobeweisaufnahmen im Zivilverfahren, jener von *Manfred Büchele* mit Fragen der Digitalisierung im Immaterialgüterrecht, *Amalia Diurni* untersucht das Thema „Human Vulnerability in Interaction with AI", *Bernhard Koch* stellt Neuerungen bei der Produkthaftung im digitalen Zeitalter vor, *Rupprecht Podzsun* und *Sarah Hinck* diskutieren die Macht in der digitalen Plattformökonomie, und *Stefano Troiano* und *Stefano Gatti* beschäftigen sich mit dem „right to data portability under the GDPR and beyond".

Einige dieser Vorträge wurden vom Institut für Italienisches Recht beigesteuert und sind in englischer Sprache verfasst, um sie der Leserin und dem Leser besser zugänglich zu machen. Wir hoffen, dadurch einen interessanten Querschnitt zu den Problemen und Fragen zu bieten, die die fortschreitende Digitalisierung und Internationalisierung in diesen Bereichen der Rechtswissenschaften aufwerfen.

Zu danken haben wir dem Dekan der Rechtswissenschaftlichen Fakultät der Universität Innsbruck, Herrn Univ.-Prof. Dr. *Walter Obwexer*, der für die Finanzierung dieses Bands gesorgt hat. Besonderer Dank gilt weiters Herrn Univ.-Ass. Mag. *Felix Rathgeb* für seinen Einsatz bei der Organisation und Erstellung des gesamten Tagungsbands sowie Frau Univ.-Ass. Mag.ª *Lena Gaggl*, Herrn Univ.-Ass. Mag. *Bernhard Hager*, Frau Univ.-Ass. Mag.ª *Maria Paulmichl* und Frau Stud.-Ass. *Leila Fasching*, die sich bei der Überarbeitung und Vereinheitlichung der Manuskripte verdient gemacht haben. Dem Verlag Mohr Siebeck und insbesondere Frau *Daniela Taudt-Wahl* und Frau *Silja Meister* möchten wir für die Drucklegung und die freundliche Betreuung danken.

Innsbruck, im Jänner 2025

*Philipp Anzenberger*
*Klaus Schwaighofer*

# Inhaltsverzeichnis

# Abkürzungsverzeichnis

| | |
|---|---|
| a. A. | andere Ansicht |
| a. a. O. | am angeführten Ort |
| a. M. | anderer Meinung |
| ABl. | Amtsblatt der Europäischen Union |
| ABoR | Administrative Board of Review |
| Abs. | Absatz |
| ACM | Autoriteit Consument en Markt |
| AGCM | Autorità garante della Concorrenza e del Mercato |
| AI | artificial intelligence |
| AIDP | Association Internationale de Droit Pénal |
| al. | alter |
| AMLA | Anti Money Laundering Authority |
| Anm. | Anmerkung |
| AnwBl | Anwaltsblatt |
| API | Application Programming Interface |
| arg. | argumentum |
| ARHG | Auslieferungs- und Rechtshilfegesetz |
| ARHV | Auslieferungs- und Rechtshilfeverordnung |
| Art. | Artikel/Article |
| Aufl. | Auflage |
| ausf. | ausführlich |
| AußStrG | Außerstreitgesetz |
| Az. | Aktenzeichen |
| BCBS | Basel Committee on Banking Supervision |
| BegrRegE | Begründung Regierungsentwurf |
| Beschl. | Beschluss |
| betrDEStA | betrauter Delegierter Europäischer Staatsanwalt |
| BGBl. | Bundesgesetzblatt |
| BGH | Bundesgerichtshof |
| BGHSt | Entscheidungen des Bundesgerichtshofs in Strafsachen |
| BiBuG | Bilanzbuchhaltungsgesetz |
| BIS | Bank for International Settlements |
| BKA | Bundeskanzleramt der Republik Österreich |
| BKartA | Bundeskartellamt |
| BlgNR | Beilagen zu den stenographischen Protokollen des Nationalrats |
| BMJ | Bundesministerium für Justiz |
| Bsp. | Beispiel |
| bspw. | beispielsweise |
| BT-Drs. | Drucksache Deutscher Bundestag |

| | |
|---|---|
| BudgetbegleitG | Budgetbegleitgesetz |
| BWG | Bankwesengesetz |
| bzw. | beziehungsweise |
| ca. | circa |
| CAC | Cyberspace Administration of China |
| CAs | conversational agents |
| CEBS | Committee of European Banking Supervisors |
| cf. | confer |
| COREPER | Ausschuss der Ständigen Vertreter |
| CRD | Capital Requirements Directive |
| CRR | Capital Requirements Regulation |
| DA | Data Act |
| DGA | Data Governance Act |
| Dir. | Directive |
| DMA | Digital Markets Act |
| DRiZ | Deutsche Richterzeitung |
| DRM | Digital Rights Management |
| DSA | Digital Services Act |
| DSG | Datenschutzgesetz |
| DS-GVO | Datenschutz-Grundverordnung |
| dZPO | deutsche Zivilprozessordnung |
| e. g. | exempli gratia |
| EBA | European Banking Authority |
| ebd. | ebenda |
| ECJ | European Court of Justice |
| ecolex | Zeitschrift für Wirtschaftsrecht |
| ed(s). | editor(s) |
| ed. | edition |
| EDIS | European Deposit Insurance Scheme |
| Edit. | Edition |
| EDPB | European Data Protection Board |
| EDPS | European Data Protection Supervisor |
| EEA | Europäische Ermittlungsanordnung |
| EG | Europäische Gemeinschaft |
| EGMR | Europäischer Gerichtshof für Menschenrechte |
| EHDS | European Health Data Space |
| EHR | electronic health records |
| Einl. | Einleitung |
| EIOPA | European Insurance and Occupational Pensions Authority |
| eJABl | Elektronisches Amtsblatt der österreichischen Justizverwaltung |
| EKHG | Eisenbahn- und Kraftfahrzeughaftpflichtgesetz |
| ELI | European Law Institute |
| EMRK | Europäische Menschenrechtskonvention |
| endg. | endgültig |
| Entsch. | Entscheidung(en) |
| Entw. | Entwurf |
| EO | Exekutionsordnung |
| ERA | Europäische Rechtsakademie |

| | |
|---|---|
| Erläut. | Erläuterungen |
| ErläutRV | Erläuterungen zur Regierungsvorlage |
| ErwGr. | Erwägungsgrund |
| ESFS | European System of Financial Supervision |
| ESMA | European Securities and Markets Authority |
| ESRB | European System Risk Board |
| EStG | Einkommensteuergesetz |
| et al. | et alter |
| etc. | et cetera |
| et seq. | et sequens |
| et seqq. | et sequentes |
| EU | Europäische Union |
| EuBagatellVO | Europäische Verordnung zur Einführung eines europäischen Verfahrens für geringfügige Forderungen |
| EuBVO | Europäische Beweisaufnahmeverordnung |
| EuDigiJustVO | Europäische Verordnung über die Digitalisierung der justiziellen Zusammenarbeit |
| EU-FinAnpG | EU-Finanz-Anpassungsgesetz |
| EuG | Gericht der Europäischen Union |
| EuGH | Europäischer Gerichtshof |
| EU-JZG | Bundesgesetz über die justizielle Zusammenarbeit in Strafsachen mit den Mitgliedstaaten der Europäischen Union |
| EU-RhÜbk | Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union |
| EUStA | Europäische Staatsanwaltschaft |
| EUStA-DG | Bundesgesetz zur Durchführung der Europäischen Staatsanwaltschaft |
| EUStA-VO | Verordnung zur Durchführung einer verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft |
| EuZW | Europäische Zeitschrift für Wirtschaftsrecht |
| EvBl | Evidenzblatt der Rechtsmittelentscheidungen der ÖJZ |
| EZB | Europäische Zentralbank |
| f. | und der/die folgende |
| Fallnr. | Fallnummer |
| ff. | und der/die folgenden |
| FM-GwG | Finanzmarkt-Geldwäschegesetz |
| Fn. | Fußnote |
| fn. | footnote |
| FRIA | Fundamental Rights Impact Assessment |
| FSE | Fascicolo Sanitario Elettronico |
| FTC | Federal Trade Commission |
| G7 | Group of Seven |
| GAFAM | Google, Apple, Facebook, Amazon und Microsoft |
| GD GROW | Generaldirektion Binnenmarkt, Industrie, Unternehmertum und KMU |
| GD JUST | Generaldirektion Justiz und Verbraucher |
| GDPR | General Data Protection Regulation |
| gem. | gemäß |

| | |
|---|---|
| ggf. | gegebenenfalls |
| GOG | Gerichtsorganisationsgesetz |
| GP | Gesetzgebungsperiode |
| GRUR Int. | Gewerblicher Rechtsschutz und Urheberrecht Internationaler Teil |
| GWB | Gesetz gegen Wettbewerbsbeschränkungen |
| h. M. | herrschende Meinung |
| HBÜ | Haager Beweisaufnahme-Übereinkommen |
| HDAB | health data access body |
| HMI | human-machine interaction |
| i. d. F. | in der Fassung |
| i. d. R. | in der Regel |
| i. e. | id es |
| i. e. S. | im engeren Sinn |
| i. S. | im Sinn von |
| i. S. d. | im Sinn des/der |
| i. V. m. | in Verbindung mit |
| i. w. S. | im weiteren Sinn |
| IBOA | institutions, bodies, offices and agencies of the EU |
| iFamZ | Interdisziplinäre Zeitschrift für Familienrecht |
| IO | Insolvenzordnung |
| IoT | Internet of Things |
| IRP | Internal Rules of Procedure |
| Iss. | Issue |
| ITS | Implementing Technical Standards |
| JBl | Juristische Blätter |
| JCA | Journal of Consumer Affairs |
| JETL | Journal of European Tort Law |
| JN | Jurisdiktionsnorm |
| JSt | Journal für Strafrecht |
| JST | Joint Supervisory Teams |
| JuBG | Justiz-Begleitgesetz |
| JusIT | Zeitschrift für IT-Recht, Rechtsinformation und Datenschutz |
| Kap. | Kapitel |
| KI | Künstliche Intelligenz |
| KMU | kleine und mittlere Unternehmen |
| KVR | Rechtsbeschwerdeverfahren in Kartell-Verwaltungssachen |
| leg. cit. | legis citatae |
| Lfg. | Lieferung |
| lit. | litera |
| LK-StPO | Linzer Kommentar zur Strafprozessordnung |
| LLM | Large Language Model |
| LoseBl | Loseblattsammlung |
| LSI | less significant institutions |
| LUISS | Libera Università Internazionale degli Studi Sociali |
| m. a. W. | mit anderen Worten |
| m. E. | meines Erachtens |
| m. n. | marginal number |
| m. w. N. | mit weiteren Nachweisen |

| | |
|---|---|
| ME | Ministerialentwurf |
| MiCA | Markets in Crypto-Assets |
| Mio. | Millionen |
| MR | Medien und Recht |
| Mrd. | Milliarden |
| MR-Int | Medien und Recht International |
| NCA | national competent authorities |
| NJW | Neue Juristische Wochenschrift |
| NJW-Beil. | Neue Juristische Wochenschrift – Beilage |
| NLG | Natural Language Generation |
| no. | number |
| NPHRL | Entwurf einer neuen Produkthaftungsrichtlinie |
| Nr. | Nummer |
| NSCAI | National Security Commission on Artificial Intelligence |
| NTF | New Technologies Formation |
| NZKart | Neue Zeitschrift für Kartellrecht |
| ÖBl | Österreichische Blätter für Gewerblichen Rechtsschutz und Urheberrecht |
| ÖBl-LS | ÖBl-Leitsätze |
| ODR | Online Dispute Resolution |
| OECD | Organisation for Economic Co-operation and Development |
| OGH | Oberster Gerichtshof |
| ÖJA | Österreichisches Juristisches Archiv |
| OJEU | Official Journal of the European Union |
| öJGG | österreichisches Jugendgerichtsgesetz |
| ÖJZ | Österreichische Juristenzeitung |
| ÖJZ-MRK | Entscheidungen zur MRK in der ÖJZ |
| OLAF | Europäisches Amt für Betrugsbekämpfung |
| OLG | Oberlandesgericht |
| öStGB | österreichisches Strafgesetzbuch |
| öStPO | österreichische Strafprozessordnung |
| OTF | Organised Trading Facility |
| öUrhG | österreichisches Urheberrechtsgesetz |
| öZPO | österreichische Zivilprozessordnung |
| para. | paragraph |
| PHRL | Produkthaftungsrichtlinie |
| PIF-Richtlinie | Richtlinie über die strafrechtliche Bekämpfung von gegen die finanziellen Interessen der Union gerichtetem Betrug |
| PIMS | personal information management systems |
| PLF | Product Liability Formation |
| PSA | Payment Services Austria |
| RDi | Recht Digital |
| rec. | recital |
| RegE | Regierungsentwurf |
| RL | Richtlinie |
| Rn. | Randnummer |
| Rs. | Rechtssache |
| RtDP | right to data portability outlined by the GDPR |

| | |
|---|---|
| RTS | Regulatory Technical Standards |
| RZ | Österreichische Richterzeitung |
| S. | Satz |
| s. | siehe |
| s. o. | siehe oben |
| SARs | socially assistive robots |
| Sec. | Section |
| sent. | sentence |
| SI | significant intsitutions |
| SME | small and medium-sized enterprises |
| SRM | Single Resolution Mechanism |
| SSM | Single Supervisory Mechanism |
| SSRN | Social Science Research Network |
| SSt | Entscheidungen des Obersten Gerichtshofs in Strafsachen und Disziplinarangelegenheiten |
| StA | Staatsanwaltschaft |
| StPRÄG | Strafprozessrechtsänderungsgesetz |
| StrEU-AG | Strafrechtliches EU-Anpassungsgesetz |
| u. a. | unter anderen/anderem |
| US | United States |
| u. U. | unter Umständen |
| UAbs. | Unterabsatz |
| UK | United Kingdom |
| UNESCO | United Nations Educational, Scientific and Cultural Organization |
| untDEStA | unterstützender Delegierter Europäischer Staatsanwalt |
| Urt. | Urteil |
| usw. | und so weiter |
| v. | von/vom |
| v. a. | vor allem |
| Vers. | Version |
| vers. | version |
| VfGH | Verfassungsgerichtshof |
| VG | Verwaltungsgericht |
| vgl. | vergleiche |
| VLP | very large platforms |
| VO | Verordnung |
| Vol. | Volume |
| VPN | Virtual Private Network |
| vs. | versus |
| WK-StPO | Wiener Kommentar zur Strafprozessordnung |
| WP29 | Article 29 Working Group on Data Protection |
| WTBG | Wirtschaftstreuhandberufsgesetz |
| Z. | Ziffer |
| z.B. | zum Beispiel |
| Zak | Zivilrecht aktuell |
| ZEuP | Zeitschrift für Europäisches Privatrecht |
| ZFR | Zeitschrift für Finanzmarktrecht |

| | |
|---|---|
| ZfRV | Zeitschrift für Europarecht, internationales Privatrecht und Rechtsvergleichung |
| ZIK | Zeitschrift für Insolvenzrecht und Kreditschutz |
| ZPD | zentraler Plattformdienst |
| ZUM | Zeitschrift für Urheber- und Medienrecht |
| zust. | zustimmend |
| ZVN | Zivilverfahrens-Novelle |
| ZWF | Zeitschrift für Wirtschafts- und Finanzstrafrecht |

# Artificial Intelligence and Criminal Law

## Challenges to Some Traditional Categories

*Lorenzo Picotti*



## I. Introduction

The challenges that technological evolution has always posed to legal formants now find a new object in the emergence of artificial intelligence. The concept embraces a multiplicity of systems, operating in the digital sphere or even in the physical world, if equipped with hardware, such as robots or self-driving vehicles, in any case interacting with human beings and the environment. Besides immeasurable benefits for individuals and the community, however, they also create new risks, due to the decision-making autonomy that characterises them to varying degrees, based on autonomous learning mechanisms from the web and the external environment. Hence a diaphragm is interposed between the act of man 'behind' such machines and their behaviour or effects, which may be 'unpredictable' and offend legal goods, including fundamental rights, deserving criminal protection: Thus, the need to adapt the criteria for attributing liability to the natural and legal persons in whose interest they

operate, while at the same time respecting the guarantee principles of criminal law, in particular of legality and of culpability. In this regard, the recommendations on substantive criminal law that the *Association Internationale de Droit Pénal* approved in the international congress held in Paris in juin 2024, dedicated to the topic of criminal justice in the face of artificial intelligence, are taken into account.

## II. The Challenges of Technological Development to Legal Formants: The Emergence of Artificial Intelligence

The challenges of technological development to criminal law have always represented a stimulus to innovation in its three recognised formants.

First of all, they prompt legislators to critically examine existing legislation, in order to fill in any gaps with new provisions, to check if they are deemed necessary to deal with unlawful or socially harmful conduct that may be manifested through new technologies or to their detriment; gaps that the prohibition of analogy should prevent jurisprudence from overcoming by way of interpretation, in the daily endeavour to respond to new cases of offence (or new ways of offence) to traditionally protected legal goods, and sometimes also to new interests that have emerged as a result of technological developments.

No less stimulating is the need to verify, on a doctrinal level, the resilience of the dogmatic categories on which the attribution or modulation of criminal liability is based, in light of phenomena that may require their adaptation or even their partial overcoming, in favour of new attribution models. And in this regard, the dilemma may arise as to whether to renounce criminal protection, considering the content of traditional categories as an insurmountable limit of punitive intervention, with possible recourse to alternative techniques of protection (of a civil or administrative nature, for example), or whether one can or must review their conceptual content, without prejudice to their systematic function, within the limits in which they express principles of guarantee and of certainty that cannot be renounced.

For some time now, such demands have emerged in view of developments in the so-called risk society that characterises our age.[1] Consider, for instance, the environment, in its various articulations and components, facing the multiple phenomena of pollution and the risks of climate change; or the risks arising from defective products or from food and drink production techniques; or, again, the risks to the rights of the individual when confronted with developments in genetics and medicine, as well as

[1] On the wide-ranging debate that has developed internationally on the relationship between criminal law and the modern risk society, see the well-known contribution of *Prittwitz*, Strafrecht und Risiko. Untersuchungen zur Krise von Strafrecht und Kriminalpolitik in der Risikogesellschaft, 2nd ed., 2021; the careful remarks of *Sieber*, The Paradigm Shift in the Global Risk Society: From Criminal Law to Global Security Law – An Analysis of the Changing Limits of Crime Control, Journal of Eastern-European Criminal Law 2016, Iss. 1, 14.

to privacy and other rights, including those of a patrimonial nature, in the face of offences and threats originating from the spread of information and communication technologies, which has characterised the last half century at the turn of the new millennium.[2]

In this context, in which a strong drive has emerged in European and international law to adapt criminal protection, which has been deemed to be extended to respond to the new threats, a further challenge is now represented by the development of artificial intelligence (henceforth: AI), due to the very rapid spread of 'systems' that, even without our clear awareness, make use of AI, both in purely digital spheres (think of search engines, which are queried on a daily basis, or the 'personalised' online offer of films, music, travel, products, advertisements, social groups to join, etc.) and in the physical world, if equipped with hardware (so-called embedded AI), such as robots or other devices, like for example self-driving cars or so-called smart weapons.

The latest developments of the so-called generative AI, of which ChatGPT is the symbol, are having a strong impact, with great expectations in public opinion and in the market. ChatGPT is capable of producing and offering new contents 'created' autonomously in response to users' questions, with which it can establish a real dialogue, including a vocal one.

There is no denying the immeasurable advantages for individuals and the community to be derived from such developments, both economically and in terms of security and efficiency of disparate services and activities, given the great speed, precision, and capacity for action and reaction, based on the gathering and processing of enormous quantities of information, acquired in real time from the web and the outside world by means of optical, acoustic and thermal sensors, etc. As a result, AI systems can not only support, but also replace humans in an increasing number of functions and activities, especially if they are dangerous or complex, or even merely repetitive, being able to respond autonomously to external stresses, including adverse events, even accidental ones, or cyber or other attacks (think of military defence systems using so-called smart weapons).

However, new risks are also emerging, which need to be adequately addressed, linked precisely to the progressive replacement of man and, therefore, to the loss of his direct and complete control over the activities gradually 'delegated' to AI systems, which are entrusted with decisions and behaviours, even of vital importance. One may think of a road accident caused by or ascribable to the autonomous driving of a vehicle, or of a surgical operation performed by a specific robot with an adverse outcome; or (entering the field of malicious conduct) of stock exchange trading managed by means of so-called high-frequency algorithms, leading to market manipulation; or even of killings or injuries to persons carried out by means of drones or other

[2] For an up-to-date overview please refer to *Picotti*, Diritto penale, tecnologie informatiche ed intelligenza artificiale: una visione d'insieme, in: Cadoppi/Canestrari/Manna/Papa (eds.), Cybercrime, 2nd ed., 2023, 32 (35 et seq.).

so-called smart weapons, capable of autonomously identifying, selecting and hitting targets, without direct control or specific command by a human being, etc.

The need for protection in the face of these and similar risks and events cannot be distinguished from those for which the legal system already offers a criminal response. To a first approximation, therefore, it cannot be accepted that they go unpunished, because the use of an AI system is involved in their realisation; all the more since their progressive diffusion would widen the gaps in protection in the near future, creating a sort of immunity for the subjects (individuals and collective entities) who design, produce, distribute, use them, in their own interest or advantage.[3]

## III. On the Essential Characteristics of AI Systems and Possible Frictions with Certain Penal Categories

The technical peculiarities of artificial intelligence highlight, however, possible frictions with well-established categories of criminal law, such as causality and culpability, on which criminal responsibility is based.

Assuming that there is no unitary and recognised legal definition of artificial intelligence, to be considered as a metaphor evocative of a plurality of different techniques and systems,[4] two elements that characterise such systems appear which are very relevant to criminal law.

The first is that such AI systems are based on multiple and increasingly sophisticated (self-)learning techniques, called machine learning (such as those based on the so-called neural networks, capable of reproducing storage mechanisms analogous to those of the human mind), with which they autonomously acquire enormous quantities of data and information of all kinds, both in cyberspace (thanks to the growing availability of data, personal and otherwise, fed by the daily activities of billions of users and entities), and in the outside world, through the aforementioned optical, acoustic, thermal sensors, etc.

The speed and power of today's connections allow their immediate gathering, selection, processing, and sharing with other systems, in accordance with the purposes pursued: thus, the information 'material' on which they are based is not (only) that provided or chosen by the human being, but is sought and identified, and in part even created, without the human's intervention – in the case of generative AI – by the systems themselves.

Relevant is the 'training' that the systems develop using increasing amounts of data and information, in order to progressively reduce error margins. One may think

[3] On this subject, please see *Picotti*, The challenges of new technologies for European criminal law, in: Luchtman (ed.), Of swords and shields: due process and crime control in times of globalization. Liber Amicorum Prof. Dr. J. A. E. Vervaele, 2023, 805, and there further bibliographical indications.

[4] A reference could now be made to Art. 3 para. 1 of the AI Act.

of facial recognition techniques, but also of moving vehicles, or objects such as road signs or obstacles in traffic, which require comparison with the maximum possible amounts of images and sounds, reproducing different faces or things of similar categories, and their parts, in different contexts.

The second relevant aspect is that, alongside and in close correlation with this cognitive profile, there is a corresponding space of autonomy of decisions, even operational ones, that AI systems are able to take, minimising time and errors, compared to what a human agent or even an organised entity based on the activity of physical persons could do; decision-making autonomy that can also be expressed in the ability of the algorithms themselves to adapt, without specific human intervention, on the basis of the experience they have acquired, which thus makes their final behaviour or output 'unpredictable' (or not entirely predictable).

Because of these characteristics, a 'will' seems to emerge in the systems themselves, distinct from that of humans, which also differentiates AI systems from common computer systems, whose functioning is based on mathematical calculations according to predefined programmes, albeit complex, moving from a determined set of data, which have long been the subject and reason for reformatory interventions in criminal legislation at the supranational and national level.[5]

The action of AI systems now raises new issues, involving philosophy and ethics, which are committed to defining its characteristics and, if possible, orienting it, distinguishing actions of AI systems from man's acting and thinking, characterised by the 'conscience' of himself and his actions, which delineates his will as the expression of a freedom (more or less extensive) of self-determination in his relations with others and with society. And it is on this freedom that moral and social, even before legal, responsibility for its own actions is based, which would not be conceivable – at least at the current stage of technological development – for AI systems as such.

Their growing autonomy of decision and behaviour does, however, create a diaphragm, in terms of causation and culpable attribution, with respect to the human act, which remains at the origin of the design, production, finalisation, and use of these systems, in a chain that is so articulated and in many places obscure (one speaks of a black box, to designate the recurring situation in which it is not possible to retrace all the steps and modalities, often unrepeatable, through which an AI system arrives at a certain output), so as to make it problematic to ascribe the 'fact' realised to the human agent – natural person or entity – who is nevertheless 'behind the machine'.[6]

---

[5] For a recent overview on the implementation of the Cybercrime Convention, if desired, see again *Picotti*, I primi vent'anni della convenzione di Budapest nell'ottica sostanzialstica e la mancata ratifica ed esecuzione del primo protocollo addizionale contro il razzismo e la xenofobia, Diritto penale e processo 2022, Iss. 8, 1028 (1028 et seq.).

[6] For a careful analysis, based on broad international literature and attentive to the technological as well as the juridical profiles of the topic, see *Giannini*, Criminal Behavior and Accountability of Artificial Intelligence Systems, 2023.

## IV. The Recommendations of the *Association Internationale de Droit Pénal* Concerning Substantive Criminal Law

The *Association Internationale de Droit Pénal* (AIDP), at the end of its last five-year Congress held in Rome at the LUISS University in 2019, decided to devote the work of the XXI. congress, held in Paris in June 2024 – on the occasion of the centenary of its foundation, which took place just a century ago in the French capital – on the topic 'Artificial Intelligence and Criminal Justice' in its different aspects. In addition to those of substantive criminal law, to which the first two sections were dedicated, dealing respectively with the general and the special part, the criminal process was also strongly involved (to which the third section was dedicated), starting with the topic of the search and collection of evidence, by means of algorithms and intelligent agents, up to the scenarios of the so-called 'predictive' justice and policing, with all the advantages and risks of entrusting to such systems – increasingly relevant – parts of the functioning of criminal justice; while important reflections also concerned the international dimension, from judicial cooperation to humanitarian law, with particular attention to the use of smart weapons (Autonomous Weapon System), to which the fourth section was devoted.

In previous years, the work of the different sections has been carried out using the 'AIDP method', based on the collection of national reports, which respond to a questionnaire formulated by the *rapporteur général* of each section, who then draws up a general report and draws up a draft resolution that is then submitted to the representatives of the various national groups who participate in a specific international Colloquium, for each section, in which the text containing the 'recommendations' that AIDP addresses to legislators, magistrates, politicians, practitioners, citizens as well as criminal law scholars, is discussed, amended, supplemented and, finally, approved, in order to propose reasonable answers to the issues addressed.

To date, all four resolutions discussed at the International Colloquia in Syracuse (September 2022) for section I, in Bucharest (June 2023) for section II, in Buenos Aires (March 2023) for section III and, most recently, in Opatija (December 2023) for section IV have been approved and are or will be available on the AIDP website.[7]

### *1. Criminal Protection Requirements for Offensive Acts Carried out through or to the Detriment of AI Systems: The Man 'Behind' the Machine*

Only the profiles of substantive criminal law can be dealt with here, starting from the recommendations approved at the outcome of the work of section I on the topic: 'Traditional criminal law categories and AI: crisis or palingenesis?'[8], supplemented

[7] Available at https://www.penal.org/ (last accessed on: 7 July 2024).

[8] The general report edited by the undersigned, the adopted resolution, and a selection of country reports are published in Revue Internationale de Droit Pénal 2023, Iss. 1, 11, 53 and 93 et seqq. respectively.

by those approved at the outcome of the work of Section II, concerning the special part.[9]

Fundamental is the recognition that the development and dissemination of AI systems, certainly desirable because they represent a formidable advance for society as a whole, constitute at the same time a new source of risks, precisely because, as they become increasingly autonomous, their operation and their outcomes may, as has been said, be 'unpredictable' even for those who design, programme, produce, distribute and use them.

Moreover, they can play a growing and increasingly insidious role as a 'tool' for committing criminal acts, facilitated or directly carried out by AI systems, as in the case of smart weapons or high-frequency algorithms.

As the fields of application broaden, the illicit or harmful acts may harm a plurality of interests, legal goods and even fundamental rights, which require adequate protection, while respecting the fundamental principles of criminal law, starting with those of legality, offensiveness, proportionality and culpability.

But the traditional models of criminal liability must be reconsidered and adapted, if necessary, to respond effectively to emerging protection needs, as already indicated by numerous supranational sources, mostly of soft law.[10]

A special definition for criminal purposes of artificial intelligence, a notion that, moreover, does not find unambiguous answers even in the IT field, did not seem to be recommended.

Rather, it is preferable to consider the specific characteristics of the various AI systems, which have different degrees of autonomy, and the legal definitions that may be provided by non-criminal sources for specific sectors, such as that of self-driving vehicles.[11]

The usefulness and appropriateness of recognising AI systems – at least at the current stage of technological development – a legal subjectivity, or penal capacity, whereby they could be direct recipients of precepts and sanctions, has been unanimously ruled out, both on account of their ontological distinction from human agents and of the impossibility of pursuing punishment against them.

---

[9] The general report edited by *Prof. F. Miró-Llinares*, the resolution approved in Bucharest, and a selection of national reports are published in Revue Internationale de Droit Pénal 2024, Iss. 1.

[10] See the 'Ethical Guidelines for Trustworthy AI' presented to the European Commission on 8 April 2019 by the High Level Expert Group; the 'Feasibility Study on a future Council of Europe Instrument on Artificial Intelligence and Criminal Law' by the European Committee on Crime Problems from 4 September 2020, and especially the European Regulation on Artificial Intelligence (cf. so-called AI Act), 2024/1689 of 13 June 2024.

[11] Regarding the rules in force in France, Germany and, experimentally, Italy, it suffices to refer to the respective national reports published in the cited issue of the Revue Internationale de Droit Pénal: *Lacaze*, French Report on Traditional Criminal Law Categories and AI, Revue de Droit Pénal 2023, Iss. 1, 153; *Beck*, German Report on Traditional Criminal Law Categories and AI, Revue de Droit Pénal 2023, Iss. 1, 195, *Barresi*, Italian Report on Traditional Criminal Law Categories and AI, Revue de Droit Pénal 2023, Iss. 1, 269.

On the one hand, AI systems do not (as of yet) have a conscious freedom of choice and evaluation of possible solutions to a practical problem or dilemma, considering, with the necessary flexibility, also the context of social and ethical relations and opportunities in which they operate; on the other hand, the threat and application of sanctions, albeit *sui generis*, would be emptied of effect by the absence of self-awareness of their existence in the past, present and future: hence even excluding the retributive function, due to the lack of a corresponding ethical-moral perception, not even those of special prevention and general prevention would be usefully pursued.

Consequently, the need arises to create or adapt models for attributing criminal liability to the various human agents (both natural persons and entities) that 'stand behind' the machine, i. e. to the actors in the various phases of its life cycle: from designers, to manufacturers, sellers, owners, deployers and end users, who decide on its concrete use, according to their interest and benefit.

But first, or at least in parallel with reforms and interventions of a penal nature, it has been hoped that legislators – at the international, national and regional level – as well as the competent authorities, will fully define, according to their respective powers, the regulation of the various fields in which AI systems operate, as paradigmatically seen in France and Germany, with reference to the circulation of self-driving vehicles (see footnote 10).

In particular, the essential technical standards, structural characteristics and operating conditions that AI systems and their components must possess before being placed on the market or becoming operational, interacting with the environment and people, should be established, also by means of preventive authorisation and control systems.

This is a pre-condition, with respect to the intervention of criminal law, which must be able to punish offences attributable to the operation or 'behaviour' of AI systems in accordance with the principle of *ultima ratio*.

However, the need for reasonable and proportionate criminal protection has been reaffirmed on the basis of the criterion, referred to above, that if offences to interests, legal goods and fundamental rights caused by AI systems were committed (entirely) by natural or legal persons, they would constitute a crime, or at least a punishable offence: hence they cannot go unpunished for the fact that they are committed by, through or even against the said systems.

### *2. Criminal Liability for the Unlawful Use of AI Systems*

The approved resolution distinguishes between hypotheses in which AI systems are used in activities that are per se unlawful, and hypotheses in which they are used in activities that are per se lawful, but from which risks or offences may arise.

In the former case, the focus is mainly on intentional conduct, which poses fewer problems in terms of attributing criminal liability, since the use of AI systems to

commit an offence does not appear conceptually different from the use of other means to achieve a criminal end.

However, two specific recommendations have been made:

The first recommendation concerns cases where the results of the system's operation are deviant from the purpose pursued by the human agent. In such cases, the principles of *aberratio ictus* and *aberratio delicti* should be applied. The mere material diversity of the injured object, on the one hand, should not, in fact, be an excuse if its characteristics are not relevant to the legal case that configures the criminal offence (the killing of one person instead of another by an intelligent weapon is not relevant to the commission of the offence of intentional homicide, since it is in any case foreseen and intended by the agent).

In the case, on the other hand, of the commission of an offence other than the one intended (the injuring of persons, rather than the damaging of military facilities), criminal liability should be based on the 'possibility of foreseeing' the different development of the action brought about by the AI system, applying the principles of culpable liability, as specified, however, in the following part of the resolution.

The second recommendation, since AI systems can be used to carry out particularly damaging or dangerous acts, in which the offence is amplified and aggravated, compared with what human conduct could produce, with consequences that are also very distant from the actions from which they originate, it is recommended to consider incriminating, as autonomous preparatory offences, conduct referable to the design, production, sale, purchase stages, having as their object the development of algorithms, software and 'malicious' systems, intended solely or principally to commit offences.

This choice of criminal policy, in line with the perspective expressed in the aforementioned European regulation on artificial intelligence (AI-Act), should be limited to AI systems or their components, that present particularly high risks to very significant legal assets (such as life, physical safety, freedom of other human beings) and only in the event of a clear, real and present danger, in accordance with the recommendations approved in the context of Section I of the 18th AIDP Congress in Istanbul in 2009, concerning 'The extension of forms of preparation for and participation in crime'.[12]

### *3. Criminal Liability Arising from the Lawful Basic Use of AI Systems*

Instead, in cases where artificial intelligence systems are used in lawful basic activities, from which, moreover, relevant offences may result, the most delicate questions arise from a criminal law perspective.

---

[12] Cf. *Picotti*, L'élargissement des formes de préparation et de participation – Rapport général, Revue Internationale de Droit Pénal 2007, Iss. 3, 355; while the text of the resolution approved in Istanbul can be read in the same Revue: Revue Internationale de Droit Pénal 2015, Iss. 1, 421.

Firstly, it must be acknowledged that, even in this field, there cannot fail to be an area of 'permitted risk', ethically or in any case socially acceptable, the extent of which depends on the concrete balance between the benefits that the recourse to AI systems guarantees and the 'adverse events' that may ensue, the elimination of which cannot be possible in absolute terms, but the reduction or containment of which must be reasonably pursued in order to make them wholly exceptional, having regard to the importance of the legal assets at stake.

This area should be defined upstream, by means of the aforementioned extra-criminal regulation, from which specific security obligations and precautionary rules should flow, to be applied in advance, right from the mentioned activities of design, development, production, sale, as well as use of AI systems.

Secondly, the adjustment of criminal liability models must overcome the frictions between the assumptions and criteria for attributing fault, traditionally understood, and the technical characteristics of AI systems, characterised by decision-making autonomy, concrete unpredictability of behaviour, opacity of output production mechanisms, complexity of the programming, development, production, updating and maintenance process, in which different subjects intervene.

The reason for this is the gradualness of the levels of automation in the different areas in which they operate – from those in which operation is 'automated' for many functions, but still allows the human agent to have significant control over the overall 'behaviour' of the systems, to those in which they are truly 'autonomous', so that human intervention can only be at a distance, in time and space, from their immediate decision-making operations – the wide structural margin of 'unpredictability' of concrete outcomes must be compensated for by resorting to appropriate models of imputation to the human agents 'behind it'.

In this regard, the imputation of 'crime' liability of legal persons could constitute a first reference, alongside those of product liability and liability for the protection of health and safety in the workplace. In these areas, which are already legally regulated and harmonised also at a European level, innovative principles have emerged to ground the imputation by way of fault of offences resulting from complex chains of contributions, active and omissive, with respect to legal rules of conduct or technical standards to be complied with, referring to the various subjects participating in a single organisation or to interrelated entities and centres.

To summarise: a prior assessment of the risks inherent in the specific lawful, but also potentially dangerous, activities that are carried out by or through AI systems must be demanded, to be contained within the limits of the permitted risk, concretely defined by correlated obligations of prevention and caution concerning the specific sources of danger represented by the types of systems and activities that are from time to time at issue.

In this way, it is also possible to outline duties to prevent offences, especially in the event of red flags or previous adverse events, to be imposed on categories of persons