INDEX

access to government evidence and exculpatory technologies
  robot-generated evidence, 142, 153–158
    investigative technologies, 158
    presumption in favor of open-source technologies, 157–158
    pretrial disclosure requirements, 153–156
    statutory privacy interests, 156–157
    trade secret privilege, 156–157
accessibility of robot-generated evidence, 168, 181–182, 191
acts and omissions, 12, 358
  programmers' liaibility, 42
actus reus, 46
  attributing criminal liability, 346–349
  criminal liability, 76
    autonomous vehicle-related crimes, 346–349
  hermeneutics of the situation, 336
  identification of, 352
  legal personhood, 348
  manslaughter (USA), 37
  programmers' liability, 26, 354
    automated weapons-related war crimes, 38–40
    autonomous vehicle-related crimes, 37–38
  voluntariness, 348–349
admissibility requirements, 147–150, 173, 186
  computer simulations, 154
adverse legal effects (EU law), 162
agency and freedom to act. *See also* anthropomorphizing robots; autonomy narrative
  autonomous vehicles and criminal liability, 346–349, 354
  liberum arbitrium indifferentiae, 347
alcohol interlock devices, 14, 107
algorithm and data-related risks
  automated weapons systems, 32–34
  autonomous vehicles, 27–30, 339–341, 355
  human input and cognitive biases, 121
  market manipulation, 300
  risk assessment models and recidivism, 243–244
  robot-asssisted verdicts in criminal matters, 98
  robot-generated evidence, 124–125, 253
  safeguards to minimize error and bias, 150–153
algorithmic appreciation, 121, 124
algorithmic aversion, 121
algorithmic knowledge, 339–341
allocation of liability, 25, 34–35, 42, 46, 120
  driverless taxis, 137
alternative dispute resolution, 97, 131–132
analytical software tools
  robot-generated evidence, 210–211, 213
anthropomorphizing robots, 113–116. *See also* autonomy narrative
  appearance
    interactive style, 119–120

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

anthropomorphizing robots (cont.)
physical embodiment, 119–120
robot faces, 118–119
interactivity or animacy robots, 116–117
physical presence and physical embodiment, 117–118
Artificial Intelligence Act (EU law), 75
assumption of liability (*Übernahmeverschulden*), 59
attributing criminal liability
actus reus, 346–349
mens rea, 349–352
robots as criminals, 75–78
automated data analysis, 248–249
automated driving systems. *See* autonomous vehicles
automated weapons systems, 5, 9
criminal liability
actus reus, 38–40
crimes against persons under ICL, 26
programmer control, 32
algorithm and data-related risks, 32–34
risks ouside, 35–36
user *versus*, 34–35
programmers' liability for harmful events, 12, 24–26
automation bias, 30
autonomous truck platooning, 325, 330, 331
autonomous vehicles, 8
actual driver and legal driver, 344–346
criminal liability
actus reus, 37–38, 346–349
mens rea, 349–352
national criminal law, 26
human liability for foreseen but unavoidable harm, 15–16
narratives, 312
arguments, 313
Singapore government, 319–330
NTSB investigation, 134–136
programmer control, 27
algorithm and data-related risks, 27–30
risks outside, 31–32
user *versus*, 30–31
programmers' liability for harmful events, 12
public opinion and safety/security concerns, 317–318
Singapore
benefits narrative, 319–321, 331
commercial narratives, 330–332
government's supportive role, 321–323
media coverage, 314–315, 318–319
public opinion studies, 314, 315–318
regulation and liability, 327–330
testing and trialing, 323–327
technology and narratology connection, 342–346
users' liability for harmful events, 23–24
autonomy narrative, 115, 281, 283, 291, 301, 306, 308
autopilot systems
liaibility for harm caused by robots, 299, 344–345, 356

biometric identifiers, 254
Law Enforcement Directive, 235
privacy concerns, 143
robot-generated evidence, 210, 215
breath-alcohol machines
safeguards to minimize error and bias, 147–149, 156
bystander behaviour
risks and failures outside of programmer control, 31, 32

categorisation of data. *See* taxonomy of robot testimony
causation, 11, 46
adequacy theories, 41
aggravation of risk, 42
but-for causation, 40–41
culpability assessments, 43
international criminal law functional obligations, 42
"meaningful human control," 44–46

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

programming and harm, 12, 40
automated weapons systems, 26, 39–40
autonomous vehicles, 31–32, 37–38
but-for/*conditio sine qua non* test, 40–41
proximate cause test, 41
teleological theory, 42
CE-certification marks
surgical robots, 68–70
cell-phones. *See* mobile phone records
Charter of Fundamental Rights of the EU, 103, 142
circumstantial evidence, 94, 112
eyewitness testimony compared, 112, 128–130
circumstantial information, 178–179, 185, 186, 190
Code of Conduct of the Swiss Medical Association, 57
cognitive biases. *See also* anthropomorphizing robots
eyewitness *versus* circumstantial evidence, 112, 128–130
collisions at sea
liability for harm caused by robots, 299
Comité Européen de Normalisation (CEN), 223
Comité Europeén de Normalisation Électrotechnique (CENELEC), 223
communications failures
risks and failures outside of programmer control, 31–32
communicative and expressive features of criminal punishment, 19–20
conditio sine qua non test, 40–41
connected devices, 205–207, 253, 262, 320. *See also* internet of things
consumer products and forensic law enforcement technologies distinguished, 197–198
Convention on Cybercrime 2001, 224
corporate criminal liability for the harmful actions of robots
criminal liability of humans for harmful events involving robots, 14
criminal liability of robots, 86
legitimacy of, 81–83
parallels with, 77–78
regulation and limitation, 84–86
legitimacy of the general concept, 79–81
organizational negligence and inadequately trained surgeons, 64
robots responsibility distinguished, 78
United States, 77–78
Court of Justice of the EU (CJEU), 103, 223
crime detection
criminal procedure, 91–92
criminal investigations, 92–93
function creep, 93–94
institutional safeguards, 96–97
criminal justice and the use of robot-generated evidence, 91, 103–107, 109, 141–144, 248–249
criminal law and criminal law theory, 5, 21
preventive dimension, 5–6
prevention of accidents, 7–9
suppression of conduct or products, 9–11
retrospective dimension, 6
criminal liability of humans for harmful events involving robots, 11–16
criminal liability of robots, 17–20
self-defence against robots, 17
criminal liability of humans for harmful events involving robots, 6
corporate liability, 14
foreseen but unavoidable harm, 15–16
intent to commit a crime, 15
manufacturers and programmers, 11–13
supervisors and users, 13–14

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

criminal liability of robots, 6, 17–18, 73–74
actus reus of robot activities, 76
"attribution of freedom as a social fact," 76–77
corporate criminal responsibility, 86
legitimacy of, 81–83
parallels with, 77–78
regulation and limitation, 84–86
functions of criminal proceedings and punishments
communicative and expressive features of criminal punishment, 19–20
deterrence, 19
legal personhood and AI devices, 74
mens rea of robot activities, 76
criminal negligence, 55
manufacturers' liability, 135
programmers' liability, 43–44
recklessness and carelessness, 350. *See also* recklessness
users' liability, 135
criminal procedure
detecting crime, 91–92
predictive policing, 91–92
reform relating to robot testimony, 188–189
criminal proceedings, 108–109
institutional safeguards, 96–97
investigations, 92–93
function creep, 93–94
risk assessment recommendation systems, 101–102
robot-assisted verdicts, 97–99
robots as defendants, 100–101
Customs Information System, 224
cybercrime, 224–225, 321

data analysis
automated data analysis, 248–249
data collection, 247, 248
Fourth Amendment standing, 259–261
General Data Protection Regulation, 231
data evaluation, 247, 248
data processing, 94, 247, 248
analytical software, 213
automated processing, 162
General Data Protection Regulation, 221–223, 230–231
Law Enforcement Directive, 232–237
Data Protection Directive (EU), 103, 230
Data Storage System for Automated Driving (DSSAD), 170, 181, 185
data storage/retention, 143, 170, 181–182, 247
deception and deceiving robots, 296–297
defence rights, 99–100, 142, 174
due process, 158, 194, 195–196
equality of arms, 227, 233, 240–241, 243, 248–249, 250
presumption of innocence, 97, 194, 227, 335
privilege against self-incrimination, 227
robot-generated evidence, 15–16, 186–187, 193–197
Denmark
historical call data records function creep, 94
deterrence, 19
digital evidence, 193–194. *See also* robot testimony at criminal trials
access and testing robot testimony, 95
access to government evidence and exculpatory technologies, 142, 153–158
accuracy, 138
analytical software tools, 210–211
biometric identifiers, 210
challenging algorithms, 124–125
circumstantial information, 178–179
court expertise, 249
creation of data
identity of creator, 213–214
permissions, 214–215
purpose of creation, 214
cross-examination, 124

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

defense's use of digital evidence, 194–196
electronic communications and social media, 201–203
endurance/resilience of data, 215
evaluative data, 177–178
factfinding processes, 142, 160–164
automation complacency, 163
consistency with principles of human-delivered justice, 163–164
human safety valves, incorporation of, 161–163
GPS chips, 253
growing importance, 239
information content, 179–180
internet of things and smart tools, 205–207
interpretation of data, 215–217
legal restrictions limiting access or use, 218
location data, 198–201
measurement data, 176–177
ownership and possession of data, 212–213
privacy implications, 217–218
raw data, 175–176
reliability of evidence, 198
reliability of robot memory, 125–128
right of contestation, 142, 158–160
robot-generated evidence
Fourth Amendment standing, 260–261
safeguards to minimize error and bias, 142, 144–153
search histories, 204
smart tools, 205–207
Fourth Amendment standing, 260–261
supportive defense evidence, 194
surveillance tools, 207–209
trustworthiness, 189–190
vendor records, 204
distribution of responsibilities. *See* allocation of liability
DNA evidence, 93, 128, 165, 197, 210
analytical software tools, 211
supportive defense evidence, 194
dolus eventualis, 44, 339, 350, 352, 355
criminal liability, 350–352, 353
intention and negligence, 351
war crimes, 44
doorbell-cameras, 197, 208
connected devices, 262
robot-generated evidence, 260–261
driving assistants
robot-generated evidence, 167–168
drones. *See* automated weapons systems
drowsiness detection, 107
driving assistant alerts, 167–168
forensic evidence generated by robots, 169–170
function creep, 94
due diligence
legitimate expectation, 50, 66, 68
negligence, 13
risk principle, 54–55
robot-assisted surgery, 58–59
certified for trust, 68–70
independent surgical robots, 61–64
remote-controlled robots, 60–61
robot warnings, 64–65
trust principle, 65–68
surgeons, 55–58
lex artis, 56–57
robot-assisted surgery, 58–70
due process, 194, 195–196. *See also* right to fair trial
defence rights, 158, 194, 195–196
Dutch Code of Criminal Procedure, 225–229, 248
duty of care
surgeons, 55–56
due diligence, 55–58
independent robots, 63–64
remote-controlled robots, 60–61

e-Evidence Regulation (draft) (EU), 246
electronic communications
robot-generated evidence, 201–203
Enlightenment narrative, 341

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

equality of arms, 240–241
defence rights, 227, 233, 240–241, 243, 248–249, 250
Erklären-Verstehen controversy, 342
EU law
adverse legal effects, 162
Charter of Fundamental Rights of the EU, 103, 142
Data Protection Directive, 103, 230
facial recognition, 105
General Data Protection Regulation, 103, 222, 230–231, 247
data collection, 231
data processing, 221–223, 230–231
Law Enforcement Directive, 222, 232, 247
biometric identifiers, 235
"competent authorities," 232–233
data processing, 232–237
fair processing principles, 233–235
implementation, 236
protection of personal data, 233–235
scope, 233
sensitive data, 235
processing data in criminal courts, 222–223
surveillance state, fear of, 103–104
Eurodac, 224
Eurojust, 225
European Convention on Human Rights (ECHR), 223
right to fair trial, 195, 227, 233
right to privacy, 103
European Telecommunications Standards Institute, 223
Europol, 225
Eurosur, 225
evaluative data, 177–178
Event Data Recorders (EDRs)
accessibility of data, 181
traceability of data, 182
evidence. *See also* digital evidence
circumstantial evidence, 94, 112, 178–179, 185, 186, 190
eyewitness testimony compared, 112, 128–130
criminal justice and the use of robot-generated evidence, 91, 103–107, 109, 141–144, 248–249
DNA evidence, 93, 128, 165, 197, 210
analytical software tools, 211
supportive defense evidence, 194
mobile phone records, 194
reliability of evidence, 242
eyewitness testimony, 126, 128, 141, 145, 208
Netherlands, 237, 240
robot-generated evidence, 125–128, 198
reproducibility of robot-generated evidence, 183
robot testimony at criminal trials, 95
accessibility of evidence, 181–182
circumstantial information, 178–179
evaluative data, 177–178
evidentiary issues, 170–172
forensic evidence generated by robots, 169–170
information content, 179–180
interpretation, 180, 181–182, 183–186
measurement data, 176–177
raw data, 175–176
reproducibility, 183
three-level approach, 183–186
traceability and chain of custody, 182
trustworthiness of robot testimony, 189–190
vetting robot testimony, 186–187, 190–191
rules of evidence
Netherlands, 237
Swiss Criminal Procedure Code, 173
United States, 145–146
safeguards to minimize error and bias
admissibility requirements, 147–150
algorithmic fairness, 150–153
breath-alcohol machines, 147–149, 156

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

robot-generated evidence, 142, 144–153
witness testimony, 145–147
standard of evidence
eyewitness testimony and circumstantial evidence compared, 112, 128–130
strength of evidence
eyewitness testimony and circumstantial evidence compared, 112, 128–130
traceability of robot-generated evidence, 182
chain of custody, 182
Event Data Recorders (EDRs), 182
"meaningful human control," 45
witness testimony
circumstantial evidence compared, 112, 128–130
importance, 239
safeguards, 145–147
standard of evidence, 112, 128–130
strength of evidence, 112, 128–130
unreliability, 126, 128, 141, 145, 208
eyewitness testimony
circumstantial evidence compared, 112, 128–130
unreliability, 126, 128, 141, 145, 208

facial recognition, 104–105, 210
analytical software tools, 211, 261
EU law, 105
international law, 105
racial biases, 125
fact-finding processes
criminal proceedings, 92–93
expert witnesses, 172
National Transportation Safety Board, 132–134
robot-generated evidence, 138–139, 142, 160–164
automation complacency, 163
consistency with principles of human-delivered justice, 163–164
human safety valves, incorporation of, 161–163
failure to correctly interpret or predict behaviour, 28–29, 32, 33–34, 74, 82–83, 135
fair process
criminal proceedings, 96–97, 105–106, 174
proportionality, 106
transparency and accountability, 106
First Additional Protocol to the Geneva Conventions, 26, 39–40
fitness devices
robot-generated evidence, 206
foreseeability of risk, 29–30, 34, 41–42, 44, 46, 352
function creep, 93–94, 171
criminal investigations, 93–94
Denmark, 94
drowsiness detection, 94
historical call data records, 94
Denmark, 94
functionality of robots
lex artis principle, 56–57, 58–59, 64, 70

Gefahrensatz (risk principle), 54–55
gender biases, 125, 151, 338
gender equality
interests or rights of individual robots, 10
General Data Protection Regulation (GDPR), 103, 222, 230–231, 247. *See also* EU law
German Constitutional Court (*Bundesverfassungsgericht*)
fair process, 174
Germany
causation
adequacy theories, 41
creation or aggravation of risk, 42
conditional intent, 14
corporate responsibility, 79–81
data storage duration, 234
Erklären-Verstehen controversy, 342
fair process, 174
German Criminal Code (StGB), 21
dolus eventualis, 44, 350–351

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

Germany (cont.)
intentional homicide, 38
manslaughter, 38
gleichgültig, 351
information content, 179
Law Enforcement Directive, 236–237
no alternative harmless action, 16
personal guilt, 18
robot-generated evidence, 142, 189
self-defence, 17
tolerance of human imperfections, 21
guilt
attributing guilt to robots, 18, 81, 100–101, 148

hacking
risks and failures outside of programmer control, 31–32, 35, 321
hermeneutics of the situation
actus reus, 336
autonomous vehicles, 336–338
mens rea, 336
outward and inward appearances of intention, 355–358
historical call data records
function creep, 94
human superiority narrative, 283
human values and morals
interests or rights of individual robots, 10

indiscriminate attacks
war crimes
automated weapons systems, 12, 36, 38–39, 44
information content, 179–180
"input" attacks
risks outside programmer control, 35
integration of knowledge, 342–346
intelligent speed assistance, 107
intention, 15
criminal liability, 349–352
appearance and intention, 356–358
dolus eventualis, 351
harmful events involving robots, 15
International Criminal Court (ICC), 26
international criminal law
automated weapons systems, 25, 26
"meaningful human control," 44–46
causation, 42
international humanitarian law
principle of distinction, 33
International Organization for Standardization, 222
internet of things, 311. *See also* connected devices
robot-generated evidence, 205–207, 253

judicial regulation, 8
Justice and Prosecution Data Act (Netherlands), 235

Law Enforcement Directive (LED), 222, 232, 247
"competent authorities," 232–233
fair processing principles, 233–235
implementation, 236
protection of personal data, 233–235
scope, 233
sensitive data, 235
legal implementation of technology, 339–342
legal personality of robots, 101, 347
criminal liability of robots, 74, 348–349
legal positivism, 341
legislative regulation, 8
soft law
standards and guidelines, 8
legitimate expectation
due diligence, 50, 66, 68
lex artis, 56–57, 58–59, 64, 67, 70
liability for harm caused by robots
robots as criminals
attributing responsibility, 75–78

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

robot responsibility and corporate reponsibility distinguished, 78
location data
robot-generated evidence, 198–201

"machine as a mere tool" narrative, 288, 291, 296–298, 299, 301, 306
machine-readable data, 175
evaluative data, 177–178
measurement data, 176–177
raw data, 175–176
manslaughter
actus reus, 37
autonomous vehicles
negligent manslaughter, 23, 26, 43–44
programmers' liability, 37–38
mens rea, 43–44
manufacturers' liability for harmful events involving robots, 11–13
autonomous vehicles, 135, 355
corporate criminal responsibility, 84–85
robot-assisted surgery, 63
market manipulation
deception and deceiving robots, 296–297
"meaningful human control," 12, 44–46, 47
traceability, 45
measurement data, 176–177
Medical Professions Act (Switzerland), 57
mens rea, 43
attributing criminal liability, 349–352
criminal responsibility, 349
culpability, 349
dolus eventualis, 44, 350–352
identification of, 352
indiscriminate attacks recklessness, 44
programmers' liability for harmful events, 43
automatic weapons systems, 44
autonomous vehicles, 43–44
purposely, knowingly, recklessly, and negligently, 349–352
mobile phone records
evidence, as, 194
smartphone ruling (Netherlands), 227–229
Model Penal Code (USA)
actus reus of manslaughter, 37
culpability
recklessness/carelessness, 350

narrative arguments and role of the government
community benefits of autonomous vehicles, 319–321
government support for autonomous vehicles, 321–323
regulation and liability, 327–330
testing and trialing autonomous vehicles, 323–327
narratives regarding human-robot interaction, 281–284
autonomous vehicles, 333
benefits narrative, 331
commercial narrative, 330–332
commercial success, 330–331
inevitability narrative, 331–332
Singapore government narrative, 319–330
autonomy narrative, 115, 281, 283, 291, 301, 306, 308
context, 287–288
human superiority narrative, 283
"machine as a mere tool" narrative, 288, 291, 296–298, 299, 301, 306
narrative defined, 289–291
unproblematic sidekick narrative, 283
National Transportation Safety Board (NTSB), 132–134
negligence, 11, 353
criminal liability, 349–352
dolus eventualis, 351
due diligence, 13, 55–58
risk principle, 54–55
programming and harm, 12, 41
negligent homicide
programmers' liaibility, 37–38
mens rea requirements, 43

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

Netherlands
criminal procedure law
digital forensics and cybercrime legislation, 224
Dutch Code of Criminal Procedure, 225–229
privacy and data protection law, 223
data processing in a criminal law context, 222–223
Justice and Prosecution Data Act, 235
legitimacy of evidence, 238
territorial jurisdiction, 239
Police Data Act, 235
reliability of evidence, 237
rules of evidence
establishing substantive truth, 237
smartphone ruling, 228–229
Norway
Robot Decision, 288–289

objective data, 245
ownership of data
robot-generated evidence, 212–213

Police Data Act (Netherlands), 235
possession of data
robot-generated evidence, 212–213
predictive policing
criminal procedure, 91–92
presumption of innocence, 97, 194
defence rights, 97, 194, 227, 335
pretrial disclosure requirements, 153–156, 194, 202
prevention of accidents, 5. *See also* regulation of safety and risk
criminal law and criminal law theory, 7–9
malfunctioning robots
regulation, 7–9
regulation, 7–9
regulation and liability, 327–330
regulation and limitation
corporate criminal respsonsibility, 84–86
principle of distinction
target identification, 33
privacy
data protection law, 107
expectation of privacy, 257
privacy as a personal good (US Const, 4th Amend), 256–261, 263–268
robot-generated evidence, 217–218
privilege against self-incrimination
defence rights, 227
programmers' liability for harmful events, 11–13
actus reus, 26, 354
automated weapons systems, 12, 24–26
algorithm and data-related risks, 32–34
distribution of responsibilities, 34–35
risks outside programmer control, 35–36
autonomous vehicles, 12, 354
algorithm and data-related risks, 27–30
automation bias (programmers and users), 30–31
risks outside programmer control, 31–32
causation, 26
criminal negligence, 43–44
mens rea, 43–44
proximate cause test, 41
Prüm Treaty, 224
psychology of HRI in litigation
anthropomorphizing robots, 113–116
appearance, 118–120
interactivity or animacy robots, 116–117
physical presence and physical embodiment, 117–118
cognitive biases, 120–121, 123–124
impact
appearance, 123
interactivity and animacy of robots, 122–123
physical presence and embodiment, 123

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

public opinion and safety/security concerns
autonomous vehicles, 317–318

quantity of data
automated search and analysis, 242–243
risk assessment models, 243

racial biases, 125
raw data, 175–176
recidivism
risk assessment models, 243–244
recklessness, 11, 14
criminal liability, 349–352, 355
appearance and recklessness, 356–358
programming and harm, 12, 41
war crimes, 44
recognition of robots' rights, 10–11
regulation of safety and risk. *See also* prevention of accidents
autonomous vehicles, 327–330
regulatory offenses, 5
prevention of accidents, 7–9
reliability of evidence, 242
eyewitness testimony, 128
Netherlands, 237, 240
robot-generated evidence, 125–128, 198
remote harms to other human beings, 10
remote-controlled robots
surgeon's liability for harmful events, 60–61
reproducibility of robot-generated evidence, 183
respondeat superior principle, 77, 80, 82, 353
right of contestation
robot-generated evidence, 142, 158–160
right to be forgotten, 215
right to bodily integrity, 8
right to dignity, 10, 96, 142
right to erasure, 215
right to fair trial, 195. *See also* due process
right to life, 8
right to privacy, 103
right to property, 8
risk principle (*Gefahrensatz*), 54–55
Road Traffic Act (Netherlands), 335, 344–345, 356
Road Traffic Act (Singapore), 328
Road Traffic Act (Switzerland), 167
robo-judges, 97–99
Robot Decision (Norway), 288–289, 291
Court of Appeal, 298–300
narratological analysis, 300–302
District Court judgment, 293–295
narratological analysis, 295–298
facts of the case, 291–292
legal causation, 293–294, 297–298, 299
market manipulation, 292–293
narratological analysis
Court of Appeal, 300–302
District Court judgment, 295–298
robot as stupid narrative, 295–297
Supreme Court, 305–306
Supreme Court, 302–305
narratological analysis, 305–306
robot defined, 1, 6–7
robot testimony at criminal trials, 95. *See also* digital evidence
circumstantial information, 178–179
evaluative data, 177–178
evidentiary issues, 170–172
forensic evidence generated by robots, 169–170
information content, 179–180
interpretation, 180
accessibility of evidence, 181–182
reproducibility, 183
three-level approach, 183–186
traceability and chain of custody, 182
measurement data, 176–177
raw data, 175–176
trustworthiness of robot testimony, 189–190
vetting robot testimony, 186–187, 190–191

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

robot-assisted surgery
due diligence, 58–59
certified for trust, 68–70
independent surgical robots, 61–64
remote-controlled robots, 60–61
robot warnings, 64–65
trust principle, 65–68
robot-generated evidence in litigation. *See* digital evidence; robot testimony at criminal trials
robots, status of
Robot Decision, 295–298
robots as victims of crime, 6, 21
Rome Statute, 26, 36, 39–40, 44

safeguards to minimize error and bias
admissibility requirements, 147–150
algorithmic fairness, 150–153
robot-generated evidence, 142, 144–153
Schengen Information System, 224
search histories
robot-generated evidence, 204
Securities Trading Act (Norway), 292
self-defence against robots, 6, 17
sex robots, 5, 10
sexual offenses
human liability for the use of a robot, 15
signal jamming
risks ouside programmer control, 35
simulation heuristic hypothesis, 112, 129
Singapore
autonomous vehicles, 319–330
benefits narrative, 319–321, 331
commercial narratives, 330–332
government narrative, 319–330
government's supportive role, 321–323
media coverage, 314–315, 318–319
public opinion studies, 314, 315–318
regulation and liability, 327–330
testing and trialing, 323–327
smart tools
digital evidence
Fourth Amendment standing, 260–261
GPS chips, 253
robot-generated evidence, 205–207
Smartphone ruling (Netherlands)
mobile phone records evidence, 227–229
social media
data ownership, 212
robot-generated evidence, 104, 195, 201–203, 217, 277
soft law, 8
standard of care, 12
standard of evidence
eyewitness testimony and circumstantial evidence compared, 112, 128–130
standing (US Const, 4th Amend)
challenges posed by emerging technologies, 265–268
exclusionary rule, 264–265
founding-era understandings, 264
privacy as a personal good, 256–261, 263–268
relationship with other Amendments, 263
state agency requirement (US Const, 4th Amend), 261–262
founding-era understanding warrant requirement, 269–270
private actor involvement, 269–274, 275–277
status of robots
Robot Decision, 295–298
strength of evidence
eyewitness testimony and circumstantial evidence compared, 112, 128–130
objective data, 245
supervisors' liability for harmful events involving robots, 13–14, 67
surgeon's criminal liability for harmful events involving robots
due diligence, 50–51, 70
surgical robots, 8, 70. *See also* robot-assisted surgery
definitions and terminology, 51–53

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

independent surgical robots, 61–64
remote-controlled robots, 60–61
surveillance footage
privacy rights, 214
supportive defense evidence, 194, 197, 209
surveillance state, fear of
EU law, 103–104
European Convention on Human Rights, 103
facial recognition, 104–105
US Constitution, 103
surveillance tools
robot-generated evidence, 207–209
Swiss Academy of Medical Sciences, 57
Swiss criminal law
due diligence obligations, 53, 54–55
lex artis principle, 59
negligence, 60
Swiss Criminal Procedure Code
rules of evidence, 173

target identification
principle of distinction, 33
taxonomy of robot testimony
circumstantial information, 178–179
evaluative data, 95, 177–178
information content, 179–180
processed data, 95, 176–177
raw data, 95, 175–176
technological neutrality, 188, 341
territorial jurisdiction
digital evidence, 239
Therapeutic Products Act (Switzerland), 59
three-level approach to interpretation of evidence, 183–184
establishing element of the offense charged, 185–186
event under examination, 185
source of evidence, 184–185
traceability of robot-generated evidence, 182
trade secret privilege, 96, 148, 156–157, 172, 211, 218
trust principle, 66
certification-based trust, 68–70
division of labour in surgery, 66–67
limitations, 66
surgical robots, application to, 67–68
task sharing among humans, 50, 66–67

Übernahmeverschulden (assumption of liability), 59
United Nations Economic Commission for Europe (UNECE)
availability and accessibility of data, 181
United Nations Institute for Disarmament Research (UNIDIR)
risks outside programmer control, 35–36
United States
corporate criminal responsibility, 77–78, 79
Model Penal Code (USA)
actus reus of manslaughter, 37
recklessness/carelessness, 350
rules of evidence, 145–146
US Constitution
Fifth Amendment, 195, 263
Fourth Amendment, 103, 254, 277
privacy, 255
standing, 256–261, 263–268
state agency requirement, 255, 261–262
Sixth Amendment, 195, 263
compulsory process, 157
right of confrontation, 159
surveillance state, fear of, 103
users' liability for harmful events, 13–14
autonomous vehicles, 23–24, 135
automation bias, 30

vendor records
robot-generated evidence, 204
verdict accuracy, 145
Vertrauensgrundsatz. *See* trust principle
Visa Information System, 224

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021

war crimes
  automated weapons systems
    directing attacks against civilians, 39
    indiscriminate attacks, 12, 36, 38–39, 44
  automated weapons-related *actus reus*, 38–40
  dolus eventualis, 44
witness testimony
  eyewitness testimony
    circumstantial evidence compared, 112, 128–130
    unreliability, 126, 128, 141, 145, 208
  importance, 239
  safeguards, 145–147
  standard of evidence, 112, 128–130
  strength of evidence, 112, 128–130

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 15 Nov 2026 at 02:00:35, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781009431453.021