

FIDES JURIDICA

BERICHT VAN DE REDACTIE

Beste lezer, daar zijn we dan weer. Ja, zelfs in de zomer werkt de redactie hard door aan jullie leesvoer. Ditmaal in een nieuw jasje. We zijn nog volop bezig met het finetunen van onze stijl, maar hopelijk is de leesbaarheid verbeterd. Veel leesplezier en tot september, in augustus nemen wij ook even vakantie.

ONDERWERPEN DEZE EDITIE

AI in de EU

Wat zijn de regels voor AI en waarom zijn ze eigenlijk gemaakt?

Innovatie jurist

Het docententeam geeft een inkijkje in het nieuwe vak: 'De innovatieve jurist'.

F-game en de grens van de wet

Gastschrijver Isabelle Gerrits over de trend van 'F-games'

Freds tip van de maand

Een aantal films over verschillende gevolgen van 'technology gone wrong'.



TECHNOLOGIE

Deze editie staat in het teken van technologie.

In het dagelijks leven wordt de rol van technologie steeds groter. Iedereen heeft voortaan een smartphone op zak en weinig bedrijven en overheidsinstanties kunnen je nog helpen zonder dat je op enige manier digitaal verbonden bent. Maar wat betekent dit eigenlijk voor ons? Met welke technologieën en innovaties hebben juristen te maken? En welke regels gelden er bijvoorbeeld voor AI? Is dat allemaal nodig? We nemen jullie mee in een deep-dive over online criminaliteit, de regels over AI en nog veel meer.

AI IN DE EU



“Artificiële intelligentie verwijst naar systemen die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie ondernemen om specifieke doelen te bereiken.”

AI IN OPKOMST

De afgelopen jaren is het gebruik van AI flink toegenomen en tegenwoordig is er zelfs sprake van commerciële AI. Sommigen gebruiken AI voor winst, anderen simpelweg voor het gemak. Tegenwoordig kom je zelfs op bijna elke app of website wel een AI-tool of chatbot tegen.

TIJD IS GELD

Het wordt dan ook steeds minder realistisch voor bedrijven om te concurreren zonder de hulp van AI vanwege de grote (economische) voordelen, bedrijven zoals ASML zien bijvoorbeeld al veel gewonnen uren voor haar juridische dienstverleners die AI implementeren¹.

ROUTINEWERK

Het gaat vaak over het tijdrovende en zelfs vermoeiend werk waar juristen mee bezig zijn, zoals jurisprudentie zoeken voor een zaak of het filtreren en samenvatten van ellenlange droge teksten. Dit soort langdurige routinetaken kunnen door AI worden geautomatiseerd of versneld wat betekent dat juristen sneller en efficiënter kunnen werken. Hierdoor blijft er meer tijd over voor de juridisch complexe vraagstukken.



*“Ik had altijd weinig tijd om geld uit te geven”
~Theo Hiddema
Advocaat*

1. Scheepers, ASML verwacht van dienstverleners inzet GPT-4, www.managementsite.nl

2. Toepassingen van AI. Kunstmatige Intelligentie (AI), Rijksinspectie Digitale Infrastructuur (RDI), www.rdi.nl

AI IN DE EU

AI IN DE PUBLIEKE SECTOR

Ook bij overheidsinstanties maken ze gebruik van AI of algoritmes voor administratief werk³. Uit onderzoek van TNO uit 2024 blijkt dat tenminste 266 verschillende AI-toepassingen gebruikt werden in de publieke sector. 105 van deze toepassingen (circa veertig procent) werden destijds op gemeentelijk niveau gehanteerd⁴. Het lijkt erop dat AI niet meer weg te denken is in Nederland. Een rechter bij de rechtbank Gelderland gebruikte ChatGPT zelfs in een recente zaak voor het bepalen van de levensduur van zonnepanelen⁵.

“De kern van het probleem was dat de rechter zijn oordeel baseerde op informatie die niet door de partijen was ingebracht, wat in strijd is met het principe van hoor en wederhoor. De rol van AI in de rechtspraak bevat zowel kansen als risico's voor uw bedrijf. Bij AI-gebruik, zoals in de zaak van de zonnepanelen, zou hetzelfde vraagstuk kunnen spelen”.⁶



Het gebruik van verschillende AI per publieke sector in 2024²

NADELEN VAN AI-GEBRUIK

De meeste mensen gebruiken tegenwoordig AI, ook op Google en andere websites zie je ze tegenwoordig eerder wel dan niet. Dat lijkt heel handig, maar er loeren soms grote gevaren om de digitale hoek. Als mensen zijn we gewend om tegenwoordig met minimale inzet antwoord te kunnen vinden online. Maar is dat antwoord wel correct? Vaak gokken we van wel en wij controleren deze informatie niet meer. En dat is begrijpelijk, als je wil weten waar een bitterbal van wordt gemaakt omdat op het terras daar ineens een discussie over begint, ga je niet ook nog kijken of de bronnen van Google wel correct zijn, dan wil je gewoon snel antwoord over je bitterbal.

3. Zandbergen, *Overheid zet steeds meer kunstmatige intelligentie in*, digitaleoverheid.nl

4. Hoekstra, Dom en Veenstra, *AI in de publieke dienstverlening III* (2024), TNO

5. Hansen, *De rol van AI in de rechtspraak: kansen en risico's voor uw bedrijf*, BedrijfsAdvocaat.nl

6. Hansen, *De rol van AI in de rechtspraak: kansen en risico's voor uw bedrijf*, BedrijfsAdvocaat.nl

AI IN DE EU

DESINFORMATIE

Nu AI in je zoekmachine vaak al bovenaan met een antwoord komt, is dat ook het antwoord wat wij als eerste gebruiken. Ook op Google is dit het geval, haar AI genaamd Gemini genereert tegenwoordig ook in Nederland meteen een antwoord op je vraag. Je merkt het misschien niet meteen, maar veel van deze antwoorden zijn gedeeltelijk fout gevormd zonder dat Gemini het door heeft. Gemini formuleert haar antwoord door middel van verschillende websites en fora als bronnen te gebruiken. Hoewel deze bronnen vaak van juiste aard zijn, maakt Gemini zelf een formulering op basis van kansberekeningen en verschillende stukjes informatie. De antwoorden worden namelijk niet gecontroleerd of beredeneerd op waarheid door de AI en zelfs grammaticaal correct samen gehecht tot een ‘voldoende’ coherent antwoord.⁷ Het resultaat: wat nou precies in die bitterbal zit, kan dus goed gebaseerd zijn op een mix van info uit De Speld en de Telegraaf.



*Google Gemini:
over de bitterbal*



*Encryptiesleutels
worden gebruikt
om de toegang tot
gevoelige
gegevens te
beveiligen*

VEILIGHEID VAN GEGEVENS

Een ander probleem waar AI bij komt kijken is veiligheid. Denk bijvoorbeeld aan die overheidsinstanties die werken met gevoelige informatie. Als de belastingdienst fraude controles uitvoert via een algoritme, mag je hopen dat dit algoritme deze informatie ook enkel en alleen zelf gebruikt en voor dat doelinde. Maar ook mensen zelf staan er niet altijd bij stil dat een bestand gedeeld met ChatGPT in principe ook indirect gedeeld wordt met anderen. De chatbots zelf zijn op dit moment ook nog maar net in staat om gevoelige informatie te herkennen.

⁷Damen en Damen, AI-antwoorden op Google “veranderen internet-spelregels revolutionair”, nos.nl

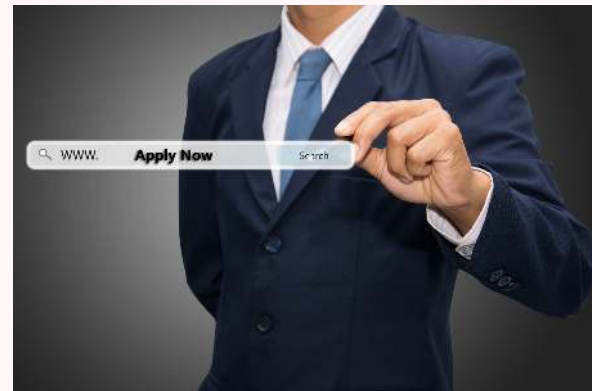
AI IN DE EU

NEGATIEVE INVLOED

De bias speelt ook een rol. AI leert van historische data die bevooroordeeld kunnen zijn. dit kan mogelijk leiden tot discriminerende of eenzijdige uitkomsten⁸. Vaak is de gebruiker zich niet bewust van zo'n bias. Het is ook vrij moeilijk vast te stellen. Veel bedrijven voeren daarom regelmatig controles uit. Als blijkt dat er enige ongewenste “vooringenomenheid” bestaat binnen de AI, dan moet deze bijgesteld worden. Het is natuurlijk geen mooi gezicht als bekend wordt dat een bedrijf discrimineert, ook al is het onbewust.

SOLLICITATIE

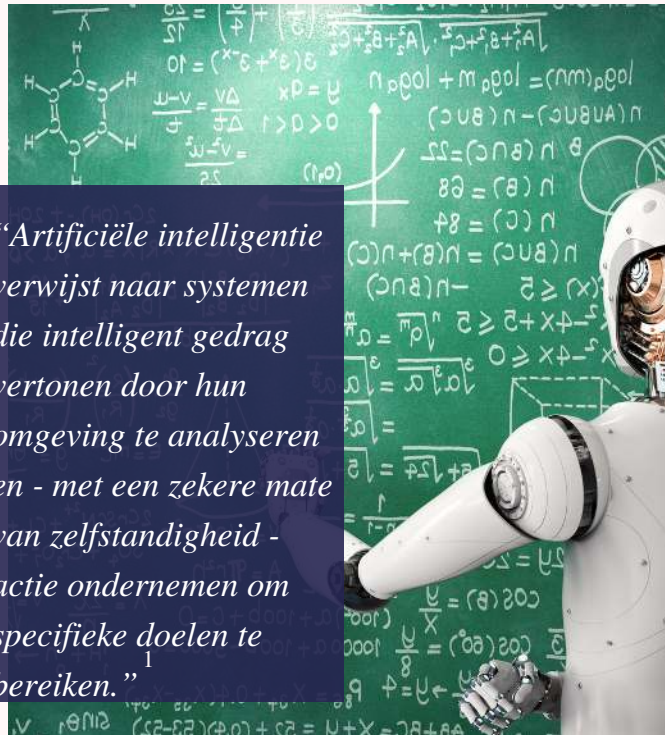
Een goed voorbeeld is de voorprocedure voor sollicitaties: Een advocatenkantoor hanteert een AI die automatische besluiten maakt, in dit geval een voorselectie om 300 sollicitaties te filteren naar 10 sollicitaties. Waar gaat de AI dan op filteren? Kans bestaat dat een AI zijn referenties online vindt. De AI wordt gevraagd om de beste sollicitanten voor een strafrecht advocaat te filteren. Dan is er een wezenlijke kans dat de AI onbewust voorkeur geeft aan mannen, als statistisch gezien mannelijke advocaten succesvoller of prominenter in het strafrecht werkzaam zijn. En als het kantoor wenst dat de sollicitant “sterk in zijn schoenen moet staan” dan is de kans bijvoorbeeld groter dat een willekeurige statistiek over confidence bij mannen en vrouwen invloed heeft.



Er zijn dus een hoop redenen waarom het gebruik van AI niet ideaal is. Toch blijft het gebruik onder personen en rechtspersonen momenteel alleen maar groeien. Het is daarom belangrijk dat we ons bewust blijven van de gevolgen en als juristen nog belangrijker om te weten wat de regels zijn en hoe dingen werken.

⁸.Automatisch besluit, Autoriteit Persoonsgegevens, <https://www.autoriteitpersoonsgegevens.nl>

DE AI-ACT



“Artificiële intelligentie verwijst naar systemen die intelligent gedrag vertonen door hun omgeving te analyseren en - met een zekere mate van zelfstandigheid - actie ondernemen om specifieke doelen te bereiken.”¹

EUROPESE UNIE

Omdat AI relatief nieuw is, is het lastig om regels te bedenken voor concepten die gedeeltelijk digitaal van aard zijn, het heeft even geduurd voordat we ook echt (geldende) AI-regelgeving hebben. Toch is Europese Unie voorloper op het gebied van deze regelgeving. Vanaf augustus 2024 geldt in de EU de AI-verordening (of AI-act). Heel goed allemaal, maar wat zijn die regels nu precies? En waarvoor dienen ze?

DOEL VAN DE AI-ACT

Het probleem is al eerder geschetst, AI wordt veel gebruikt, maar het is niet altijd verantwoord. Zwaarwegende keuzes zoals bij de Rechtbank Gelderland of het voorbeeld van de sollicitatie zijn misschien beter af zonder. Fundamentele mensenrechten komen soms ook in geding, denk bijvoorbeeld aan het recht op privacy dat geschonden wordt omdat een AI je persoonsgegevens gebruikt. De AI-act heeft als doel om al deze situaties te voorkomen en mensenrechten te beschermen.

1. Toepassingen van AI, Rijksinspectie Digitale Infrastructuur, <https://www.rdi.nl>



Het Europees Parlement te Brussel, waar onder meer de Europese Commissie en de Raad van Europa haar zitplaats hebben

DE AI-ACT

VERORDENING

Om uit te leggen hoe de AI-act werkt moeten we eerst kijken naar de bron. De AI-act is dus een Europese verordening. Anders dan andere soorten regels die vanuit de Europese Unie kunnen voortvloeien geldt voor een verordening een rechtstreekse werking (geen sprake van omzetting in nationaal regels). Daarnaast gelden verordening ook meteen tegenover iedereen, in dit geval wil dat zeggen ieder persoon, iedere organisatie én ieder land (als rechtspersoon).



Op 21 april 2021 bracht de Europese Commissie haar eerste voorstel uit voor AI regelgeving

DE REGELS

de AI-act op zichzelf is ruim honderd pagina's lang, maar is vrij overzichtelijk opgebouwd, hiernaast staat lijst die een algemeen beeld schetst van de AI-act. Er staan nog veel meer onderwerpen die de handhavende en controlerende organisaties aanstellen, maar dat is voor nu iets te droge stof. Wil je er meer over lezen? Ga dan naar de website: artificialintelligenceact.eu daar vind je alles van samenvattingen tot de exacte regels.

Voor nu beperken we ons tot de grote lijnen, namelijk:

- De transparantie- en andere plichten voor providers en gebruikers;
- De soorten AI

We behandelen deze twee onderwerpen omdat zij een aantal van de voornaamste doelen van de AI-act tackelen. Het bevorderen van de veiligheid van inwoners, bekwaamheid van de gebruiker/provider en het bewustzijn van de gevaren en risico's van AI.

Onderwerpen AI-act:

- Definities en reikwijdte van de AI-act
- Soorten AI
 - verboden varianten
 - hoog-risico varianten
 - laag-risico varianten
 - varianten met een beperkte functie
- Transparantie- en andere plichten
 - voor gebruikers
 - voor providers
- Extra regels voor general-purpose AI
- Handhaving door nationale organen
- Handhaving door de EU
- Boetes en strafbepalingen

AI-ACT

TRANSPARANTIEPLICHT

In veel opzichten is de AI-act in gelijke manier ingericht als de AVG. Er zijn verplichtingen voor de AI zoals die er zijn voor het verwerken van (persoons-)gegevens. Maar ook voorschriften voor de gebruiker, degene die gegevens deelt, of de provider, degene die de AI verschaft.

Een van de belangrijkste plichten die we in allebei terugvinden, gaat dus over transparantie. De regels in de AVG houden in dat heel concreet en afbakenend moet worden omschreven hoe de gegevens mogen worden gebruikt en waarvoor.

Het vereist onder andere voor een gegevensverwerker:

- Een duidelijke omschrijving van alle gegevens die gebruikt worden;
- Welke programma's en platformen de verwerker zal gebruiken;
- Voor welke doeleinden de gegevens worden verstrekt.

Voor de AI-act geldt dus dezelfde denkwijze, vereist is:

- Een duidelijk inzicht in de werkwijze van de AI;
- De toegang, kennis en bronnen die AI zelf gebruikt;
- Hoe en op welke manier AI gegevens gebruikt worden.



Een goed voorbeeld waar gegevensbescherming van belang is: cookies

ANDERE PLICHTEN

Andere plichten zijn bijvoorbeeld de plicht om verantwoording af te leggen aan de 'AI-autoriteiten' zoals die bepaald zijn in de verordening. Zo bestaat het Europese AI-Office, wat onder meer de kwaliteit van AI ontwikkelingen waarborgt.²

².European AI Office, Europese Commissie, digital-strategy.ec.europa.eu

AI-ACT

Emotieregulatie, het scannen en anticiperen van emoties, is ten strengste verboden op grond van de AI-act



SOORTEN AI

Voor het gebruik van AI is weer een parallel te trekken met de AVG. Degene die gebruikmaakt van AI of een verwerker is, is zelf verantwoordelijk voor de gegevens die hij/zij al dan niet deelt. Het verschil met een verwerker is echter dat deze onderscheid kan maken tussen noodzakelijke gegevens en overbodig ontvangen gegevens. Omdat een AI dit onderscheid niet kan maken, is de kans groot dat alle gedeelde gegevens ook verwerkt en verspreid worden, wat dus kan leiden tot een ernstige datalek. Daarom bestaan in de AI-act de risicocategorieën, iedere categorie geeft weer welke maatregelen er genomen moeten worden zodat het gebruik niet leidt tot problemen. De vijf categorieën zijn³:

- Verboden AI, dit zijn de AI die direct inbreuk maken op mensenrechten of malafide doeleinden kennen zoals manipulatie of emotieregulatie van mensen;
- Hoog-risico AI. Een AI die bijvoorbeeld gebruikt wordt voor beslissingen met grote (rechts)gevolgen. Denk aan het voorbeeld van de rechtbank Gelderland.
- Transparantieplichtige AI. Dit is bijvoorbeeld een chatbot, die zijn bronnen moet delen.
- Laag-risico AI, een AI die een simpele taak uitvoert maar wel zelfstandig te werk gaat, denk aan automatische updates uitvoeren in apparatuur.
- AI-modellen voor algemene doeleinden, ofwel “general-purpose AI”. Zoals de naam impliceert is deze laatste soort bedoelt om gebruikt te kunnen worden voor vrij algemene soms simpele taken/vragen. Ze hebben vaak een heel breed scala aan informatie tot beschikking en zijn in staat om zelfstandig te verbeteren en te leren door de informatie te gebruiken.

Elke soort AI komt met zijn eigen set regels en voorschriften. Ook heeft de EU verzorgd in kwalificatiekaders en zwarte lijsten voor AI zodat mensen goed begrijpen welke AI wat kan en mag. Op deze manier handhaaft de EU het gebruik van AI zodat we er samen op vooruit kunnen zonder dat mensenrechten of andere belangen in gevaar komen.

3. Nieuwe AI-regels voor ondernemers (AI Act), Rijksdienst voor Ondernemend Nederland (RVO), ondernemersplein.overheid.nl

INNOVATIEVE JURIST

NIEUW VAK

Onze opleiding kent sinds kort ook een vak over technologie en innovatie. Wij hebben daarom gevraagd aan de docenten om een stukje te schrijven. Zij geven ons een kijkje in dit gloednieuwe vak.

INPELEN OP DIGITALISERING EN BEROEPSONTWIKKELING

De module: 'De Innovatieve Jurist' is opgezet vanuit de noodzaak om toekomstgerichte juristen op te leiden in lijn met de voortdurende innovatie binnen het juridische werkveld. We zijn daarbij aangesloten bij het bredere koersbeeld van de HAN (Slim, Schoon en Sociaal), waarin digitalisering een prominente rol speelt. Ook hebben we rekening gehouden met de aanpassing van het landelijke beroeps- en opleidingsprofiel van de HBO-jurist, waarin meer aandacht is voor digitalisering als afzonderlijke competentie.



AI-GELETTERDHEID: ONMISBAAR VOOR DE JURIST VAN DE TOEKOMST

We hebben dit jaar bij de start van de module gemerkt dat studenten over het algemeen digitaal vaardig zijn en in hun studie en dagelijks leven al gebruik van AI, vooral van ChatGPT. Wat echter vaak ontbreekt, is een kritische houding en een basisbegrip van hoe AI daadwerkelijk werkt en welke risico's eraan verbonden zijn. Niet iedereen is zogenaamd: AI-geletterd, maar sinds februari 2025 verlangt de Europese AI Act dat wel van ons. Onze module speelt hierop in door studenten bewust te maken van de kansen én gevaren van het gebruik van AI binnen het juridisch domein en hen te leren hoe ze zich als toekomstbestendige professionals tot deze technologie kunnen verhouden.

INNOVATIEVE JURIST

THEMA'S

In het vak staan thema's centraal zoals digitale transformatie, recht en digitalisering, datamanagement en ethiek. Studenten leren in de basis hoe generatieve AI werkt en op welke manier je met of zonder AI innovaties kunt doorvoeren in een juridische omgevingen. Denk bijvoorbeeld aan een digitale beslisboom over een gemeentelijke regeling. Daarnaast wordt er aandacht besteed aan de juridische kaders, zoals de AVG en de AI-act. Ze leren kritisch te reflecteren op algoritmische besluitvorming en ethische dilemma's.

Onderwerpen als bias in data, transparantie, verantwoordelijkheid en toezicht komen uitgebreid aan bod. Ook wordt gewerkt aan praktische vaardigheden, zoals het beoordelen van dataset of het schrijven van een juridisch advies over een vraagstuk dat raakt aan digitalisering en recht. Hierbij mogen studenten natuurlijk AI gebruiken. Bij de toetsing hebben we daarover vervolgens een inhoudelijk (en soms kritisch) gesprek. Deze gesprekken en discussies leveren vaak verrassende inzichten op!



We denken dat een module als deze (waarin technologie, recht en ethiek met elkaar verbonden worden) belangrijk is. Juist nu de ontwikkelingen op het gebied van digitalisering bijna niet bij te houden zijn en er steeds meer Europese wetgeving op dit terrein bijkomt. In het juridische werkveld wordt daarnaast in rap tempo verkend welke juridische werkzaamheden door AI kunnen worden ondersteund of overgenomen. Ook voor ons als docenten is zo'n nieuwe module een leerproces. Uiteraard maken wij zelf ook regelmatig gebruik van AI bij het ontwikkelen van onderwijs en onderwijsmateriaal en merken we hoe belangrijk het is om kritisch te blijven op de resultaten, maar natuurlijk hebben we ons voor dit tekstje ook laten ondersteunen door AI. Het docententeam: Martijn Hendriks, Carlo Lo Manto en Ellen Lakens-van Veldhoven.

F-GAMES



CYBERCRIMINALITEIT

Op het eerste gezicht lijken F-games iets onschuldigs. Denk aan een nieuwe videogame, een populaire trend of een grappige online challenge. Maar achter deze naam schuilt helaas een verontrustende werkelijkheid: een digitale wereld waarin jongeren worden verleid tot fraude, oplichting en witwaspraktijken. Deze vorm van cybercriminaliteit wordt op sluwe wijze genormaliseerd en zelfs verheerlijkt. Luxegoederen, snel geld en status worden voorgespiegeld als haalbaar voor iedereen die deze wereld toetreedt. Jongeren raken verstrikt in een spel dat allesbehalve onschuldig is.

Wat opvallend is, is dat het aantal cybercrimezaken in Nederland schrikbarend toeneemt. Bijna de helft van deze verdachten zijn onder de 21 jaar¹. De meeste slachtoffers hebben geen idee wie er achter de schermen zitten wanneer hun gegevens worden misbruikt. Wat verklaart de groeiende populariteit van F-games onder jongeren in Nederland en wat zijn de maatschappelijke gevolgen hiervan? In dit essay worden de kenmerken van F-games onderzocht, de impact op jongeren belicht en kijk ik naar de rol van de overheid in het bestrijden van dit snelgroeiende fenomeen.



1. Mensen oplichting voor F-game | De waarheid over online fraude', NOSSstories, www.youtube.com

F-GAMES

OVER F-GAMES

Wat zijn F-games precies, welke kenmerken hiervan spreken specifiek jongeren aan en dragen daardoor bij aan de populariteit? Het is natuurlijk belangrijk om te weten wat F-games nou zo populair maakt.

Sociale media zijn voor iedereen die dat wil bereikbaar. Jongeren kunnen makkelijk in de cybercriminaliteit rollen door een combinatie van onwetendheid, de toegankelijkheid van online-tools om fraude mee te plegen en een gebrek aan bewustzijn over de consequenties van hun daden. Via drill-rap en sociale media worden F-games verheerlijkt en genormaliseerd. Hierdoor krijgen jongeren zowel bewust, als onbewust, vaak te maken met de F-games.²

FRAUDEZAKEN

Er zijn al verschillende rechtszaken geweest waarbij de rechter wordt geconfronteerd met deze manier van fraude. De Rechtbank Noord-Nederland heeft op 31 oktober 2023 een uitspraak gedaan in een strafzaak waarin de verdachte zich schuldig had gemaakt aan F-games. Deze verdachte uit 2002 heeft in een korte periode 20 personen slachtoffer gemaakt van bankhelpdeskfraude. Op de in beslag genomen telefoon is een script gevonden waar de verdachte zich aan moest houden om de fraude zo goed mogelijk te laten verlopen.³ Achter deze praktijken bevond zich een organisatie van verschillende personen. Zo was er een “collega” die het telefoongesprek met het slachtoffer voerde en hierbij aangaf dat er een andere collega in de buurt is die kan helpen om het zogenaamde probleem voor hen op te lossen. Slachtoffers waren allemaal tussen de 70 en 90 jaar oud. Elke keer werd een bijna identieke werkwijze gebruikt om zo veel mogelijk slachtoffers buit te maken.⁴

Opvallend is ook dat deze verdachte(n) communiceren via de app Signal. Het grootste voordeel van het gebruik van deze app is de privacy. Signal wil namelijk bewijzen dat privacy in de digitale communicatie een standaard is. Zij versleutelen namelijk de gegevens waardoor zij zelf, maar ook anderen, geen berichten kunnen lezen of oproepen kunnen beluisteren die niet van hen zijn.⁵



2. Van der Beek, *Zo belanden jongeren in de cybercriminaliteit*, Computable 12 juli 2024

3. Rb. Noord-Nederland, 17 oktober 2023, ECLI:NL:RBNNE:2023:4435 (bewijsoverweging wettig bewijs, eerste alinea)

4. Rb. Noord-Nederland, 17 oktober 2023, ECLI:NL:RBNNE:2023:4435, (bewijsoverweging wettig bewijs, eerste alinea)

5. Grate, *Signal app: dit zijn de voor- en nadelen. Voorlichting op Scholen*, <https://voorlichtingopscholen.nl>

F-GAMES

IMPACT OP JONGEREN

Door de toename van sociale media in het afgelopen decennium, zie je dat er veel waarde wordt gehecht aan het hebben van status. Op sociale media wordt gedeeld hoe men dure spullen, VIP-tafels in de clubs en dikke auto's hebben. Ook foto's met bekende voetballers en rappers worden gedeeld om te laten zien dat mensen ertoe doen. Hierdoor kijken jongeren naar deze mensen op en kunnen worden verleid om ook in de F-games te stappen.⁶

Sociale media spelen een grote rol in het leven van jongeren. Ze krijgen er op jonge leeftijd al veel mee te maken en maken er tegenwoordig dagelijks gebruik van. Een team communicatiewetenschappers aan de universiteit van Amsterdam hebben de impact van sociale media gebruik op jongeren onderzocht. Daar kwamen een aantal belangrijke punten naar voren. Een van die punten is dat 60% van de jongeren aangeeft dat ze overwegend negatieve gevolgen ervaren door het gebruik van sociale media. Dit met onder anderen hun zelfvertrouwen, welzijn en in de relaties met hun omgeving.⁷

6. Nieuws & Co, *Steeds meer jongeren vallen voor online oplichting: hoe voorkom je dit?*, NPO Radio 1 (6 december 2024)

7. Van der Wal, Beyens, Janssen en Valkenburg, *Social media use leads to negative mental health outcomes for most adolescents*, p. 16



Op sociale media wordt investeren in crypto's en NFT's steeds vaker gepromoot door influencers. In veel gevallen is dit een marketingstunt maar soms is het simpelweg een scam. Hoewel sommige influencers onbewust meedoen, hebben ook een aantal openlijk verklaart bewust mensen te laten investeren en dan zelf de winst tot zich te nemen. De term “rug-pull” wordt vaak gebruikt om deze acties te omschrijven online.

F-GAMES

*Het Initium
gebouw van De
Vrije Universiteit
van Amsterdam,
waar het NSCR
zich bevindt*



ONDERZOEK

Het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving heeft in oktober 2024 een onderzoek gedaan of sociale media tot meer jeugdcriminaliteit leidt. Er zijn hier verschillende voor- en tegenargumenten opgenomen. Waarbij zij aan de ene kan aangeven dat sociale media als hulpmiddel kan bieden voor de jeugdcriminaliteit omdat jongeren hier via platforms zoals Snapchat en TikTok verleid kunnen worden tot bijvoorbeeld het uithalen van drugs of het fungeren als geldezel.⁸

Aan de andere kant belichten ze ook dat sociale media de jongeren van de straat kunnen houden. De behoefte van spanning wordt online vervuld. Wat men vaak zag, was dat er veel criminaliteit ontstaat wanneer jongeren op straat rondhangen en zich vervelen, wat als trigger kan werken. Ook geven ze aan dat sociale media positief en sociaal gedrag kunnen versterken. Het maakt het voor jongeren makkelijker om contacten te kunnen onderhouden met hun leeftijdsgenoten. Sociale media biedt een laagdrempelige manier om gelijkgestemden te vinden, steun te ervaren en relevante informatie te vergaren.⁹

Al met al zijn er verschillende aanwijzingen die bevestigen, maar ook tegenspreken, dat sociale media kunnen leiden tot (meer) jeugdcriminaliteit. De invloed die de media kan hebben, verschilt volgens het onderzoek ook van persoon tot persoon. Denk hierbij aan het sociale netwerk van jongeren en natuurlijk de werking van algoritmes. Als men zich al in een omgeving bevindt waar veel criminaliteit speelt, is de kans groter dat je door verschillende algoritmes sneller op de donkere kant van sociale media terecht komt.¹⁰

8.Hoeben, Weerman en Weulen Kranenbarg, *Leiden sociale media tot meer jeugdcriminaliteit?*, NSCR Factsheet, oktober 2024, p. 1

9.Hoeben, Weerman en Weulen Kranenbarg, *Leiden sociale media tot meer jeugdcriminaliteit?*, NSCR Factsheet, oktober 2024, p. 2

10.Hoeben, Weerman en Weulen Kranenbarg, *Leiden sociale media tot meer jeugdcriminaliteit?*, NSCR Factsheet, oktober 2024, p. 5

F-GAMES

DE ROL VAN DE OVERHEID

In januari 2025 is er door de politie een onderzoek gepubliceerd naar hybride straatgeweld onder jongeren. Er wordt namelijk gezien dat geweld onder jongeren steeds vaker online componenten heeft. Gezien er nog weinig bekend is over de groei van cybercriminaliteit onder jongeren, hebben zij dit onderzoek uitgevoerd. Aan de hand daarvan zijn er verschillende aanbevelingen gedaan om inzichtelijk te krijgen hoe instanties zich kunnen voorbereiden op de groei van cybercriminaliteit onder jongeren.¹¹

De politie en andere instanties richten zich al enige tijd op het tegengaan van jonge aanwas in de georganiseerde criminaliteit, vooral bij jongeren die uit kwetsbare wijken komen. Als het gaat om hybride straatgeweld, is er vaak geen directe link met georganiseerde misdaad. Toch zijn de impact en ernst van dit soort incidenten groot genoeg om meer aandacht te vragen. Het maakt het namelijk lastig dat jongeren dit soort geweld niet melden. Daardoor hebben de instanties vaak geen inzicht op het aantal incidenten. Het is dus belangrijk dat jeugdagenten samen gaan werken met digitale experts. Dit is nodig doordat de jongeren steeds meer online leven, daar ontstaan dan ook de eerste signalen van problemen.



Op dit moment krijgen jeugdagenten nog weinig digitale ondersteuning, dit terwijl de digitale specialisten vaak niet specifiek op jeugd en geweld gericht zijn. Er is behoefte aan een betere samenwerking van online kennis met wat er op straat gebeurt.¹²

11.Mehlbaum, Van den Akker, Broekhuizen en Verweij, *Geklapt, gefilmd en gedeeld. Een onderzoek naar hybride straatgeweld onder jongeren*, Politiekunde 126, Politie & Wetenschap, januari 2025, p. 13

12.Mehlbaum, Van den Akker, Broekhuizen en Verweij, *Geklapt, gefilmd en gedeeld. Een onderzoek naar hybride straatgeweld onder jongeren*, Politiekunde 126, Politie & Wetenschap, januari 2025, p. 108

F-GAMES

LOKALE HULP

Ook is het belangrijk dat er wordt gewerkt aan een relatie met de jongeren. Het is namelijk bekend dat jongeren niet snel over hun eigen slachtofferschap willen praten met de politie. Echter blijkt het wel dat jongeren soms bereid zijn om over andere slachtoffers te praten. Door het opbouwen van een vertrouwensrelatie is het mogelijk dat de politie eerder online geweld kan signaleren. Verder wordt er ook aanbevolen dat er meer moet worden gericht op voorlichting, ondersteuning, trainingen en laagdrempelige meldpunten voor zowel ouders als jongeren.¹³

LANDELIJKE AANPAK

Naast dat het belangrijk is dat de er een lokale aanpak komt, moet de rijksoverheid ook zijn verantwoordelijkheid nemen. De ervaring leert dat socialemediaplatforms niet altijd hun verantwoordelijkheid nemen om het delen van illegale content tegen te gaan en jongeren hiertegen te beschermen. Het is daarom extra belangrijk dat de overheid afspraken maakt met deze bedrijven om de veiligheid beter te waarborgen.¹⁴ Hoewel er in Nederland wetten bestaan zoals de Wet Aansprakelijkheid voor Online Platforms en de Wet Computercriminaliteit III, blijkt in de praktijk dat deze onvoldoende effect hebben op het terugdringen van online criminaliteit onder jongeren. Volgens artikel 4 van de Wet Aansprakelijkheid voor Online Platforms zijn platforms verplicht om maatregelen te nemen tegen schadelijke en illegale inhoud, en moeten ze gebruikers beschermen tegen strafbare handelingen zoals fraude.¹⁵



POLITIE.NL:

“Ben jij slachtoffer geworden, schaam je dan niet. Je bent echt niet de enige die dit overkomt. Neem daarom altijd direct contact op met je bank om je rekening te laten blokkeren. En doe altijd aangifte bij de politie. Dat kan telefonisch, persoonlijk op het bureau of in veel gevallen ook online.

Deel daarnaast je verhaal met vrienden en kennissen. Zo help je voorkomen dat er nieuwe

13. Mehlbaum, Van den Akker, Broekhuizen en Verweij, *Geklapt, gefilmd en gedeeld. Een onderzoek naar hybride straatgeweld onder jongeren*, Politiekunde 126, Politie & Wetenschap, januari 2025, p. 109-111

14. Mehlbaum, Van den Akker, Broekhuizen en Verweij, *Geklapt, gefilmd en gedeeld. Een onderzoek naar hybride straatgeweld onder jongeren*, Politiekunde 126, Politie & Wetenschap, januari 2025, p. 113

15. Artikel 4 Wet Aansprakelijkheid voor Online Platforms

16. *Wat zijn F-games?*, politie.nl

F-GAMES

WETTELIJKE PLICHT

Daarnaast verplicht artikel 2 en 3 van de Wet Computercriminaliteit III internetbedrijven en sociale media om verdachte activiteiten, zoals online oplichting en hackpraktijken, actief op te sporen en te melden aan opsporingsinstanties¹⁷. Echter blijkt dat deze regels in de praktijk vaak nauwelijks consequenties hebben wanneer ze worden genegeerd. Criminele activiteiten zoals F-games, waarbij jongeren worden geronseld via Telegram of Snapchat om als geldezel of pinner te fungeren, blijven zich ongehinderd verspreiden. De pakkans blijkt laag en platforms grijpen zelden tijdig in. Zolang het naleven van deze verplichtingen niet steviger wordt afgedwongen, blijven jongeren een makkelijk doelwit en zal deze vorm van online criminaliteit een groeiend probleem blijven.

CONCLUSIE

Al met al kunnen we concluderen dat er vanuit het perspectief van de overheid nog werk aan de winkel is. Het komt nog te vaak voor dat socialemediaplatforms zich niet houden aan de regels omtrent illegale content, zonder dat daar echte consequenties aan verbonden zijn. Jongeren worden ondertussen steeds vaker blootgesteld aan verheerlijkte beelden van F-games, waarin snel geld, status en luxe centraal staan. De grens tussen online vermaak en strafbaar gedrag vervaagt, met alle gevolgen van dien. Hoewel er al initiatieven zijn om jongeren te beschermen en meer inzicht te krijgen in cybercriminaliteit, schieten deze maatregelen in de praktijk vaak tekort. Voorlichting, betere samenwerking tussen jeugdagenten en digitale experts én striktere handhaving van wetgeving zijn essentieel om dit groeiende probleem tegen te gaan. Want zolang jongeren met één klik in de wereld van F-games kunnen belanden, blijft het dweilen met de kraan open.

17. Artikel 2 en 3 Wet Computercriminaliteit III



*Geschreven door:
Isabelle Gerrits*

Isabelle is vierdejaars student aan de HAN en zal komend jaar afstuderen. Ze is al een tijdje werkzaam bij Stichting Achmea Rechtsbijstand. We willen Isabelle nogmaals enorm bedanken voor het schrijven van dit stuk.

FRED'S KIJKTIP

SCIENCE-FICTION OF REALITEIT

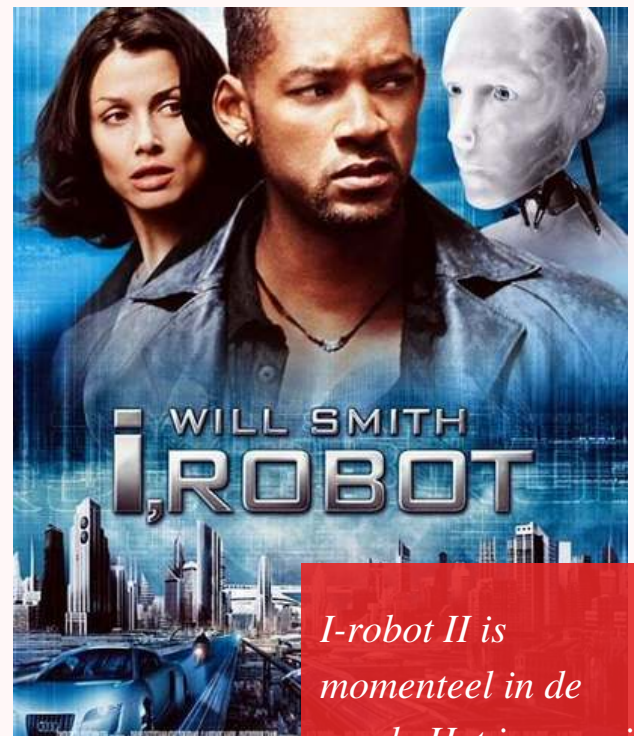
Wij als mensen zijn in onze geschiedenis nu in het hoofdstuk van de onlinetijd (zoals de steentijd) en treden net een nieuw interessante paragraaf in genaamd: “AI-era”. En zoals in elk tijdperk is er een hoop speculatie geweest over hoe de wereld er nu uit zou zien op het gebied van technologie. Helaas nog geen zwevende auto’s, maar wel Artificial Intelligence en kwantumcomputers. Om deze editie wat luchtig te houden leek het ons daarom leuk om ook een artikel te wijden aan speculatie. We nemen je mee terug in de tijd en kijken naar films en series die over AI, technologie en de toekomst gingen, ofja ons heden.

I-ROBOT, 2004

Uit het niets kwam enkele maanden ineens de trailer voor een vervolgfilm, maar voor nu even deze klassieker uit 2004, 21 jaar oud. Deze film is mogelijk ouder dan onze voorzitter, maar toch houdt deze film goed stand in de huidige media.

De film vertelt het verhaal van agent Spooner, gespeeld door Will Smith, die leeft in een toekomst waarin robots en mensen samenleven. De robots zijn geprogrammeerd om mensen te helpen en zouden mensen ook geen kwaad kunnen doen. Toch blijkt er iets niet helemaal te kloppen als verschillende ongevallen opduiken en de enige ‘mogelijke’ verdachte robots lijken te zijn.

De film zet men aan het denken over de voor- en nadelen van zulke geavanceerde technologie en over de mogelijke gevaren van zelfdenkende AI. Wil je de nog donkerde fictieve toekomst in kijken dan raad ik je aan: de Terminator-series, M3gan en natuurlijk niet te vergeten: The Matrix.



I-robot II is momenteel in de maak. Het is nog niet bekend wanneer de vervolgfilm uitkomt.

FRED'S KIJKTIP



De 6+ film is een geweldig leuke film voor jong en oud die je echt niet kan missen. Maar Wall-E brengt ook een belangrijke boodschap over de verantwoordelijkheid van de mens voor haar klimaat en eigen toekomst.

WALL-E, 2008

Vier jaar later kwam deze film uit die misschien wel lijnrecht tegenover het concept van I-Robot staat. Wederom een setting waarin robots en mensen samenleven, maar dit keer zijn de robots goedaardig. De film gaat over een eigenwijs afvalrobotje genaamd Wall-E die op aarde is met als enige doel om afval te verwerken. Nadat hij een andere robot ontmoet en volgt naar een ruimteschip zien we hoe de mensen van de toekomst leven. Ze leven niet meer op aarde en zijn enorm verwend en out-of-shape. De komst van Wall-E brengt een hoop gevolgen met zich mee, zeker als men erachter komt wat hij verborgen heeft in zijn robotbuik.

DEEP WEB, 2015

Wil je iets meer van deze tijd of iets meer juridisch relevant? Dan is Deep Web iets voor jou. In deze documentaire volgen we het verhaal van Ross Ulbricht, een jonge 'entrepreneur' die op gegeven moment Silk Road opricht. Silk Road is een van de eerste moderne zwarte markten van het internet, waarop in enorme getalen gehandeld werd in drugs. In dit waargebeurde verhaal, met bijna alle echte personen in de documentaire zie je hoe de FBI Ulbricht proberen op te sporen en Silk Road proberen te ontmantelen in een tijdperk waarin het internet nog niet gereguleerd was en een hele hoop illegale dingen verstoep waren op het web. Ook krijg je een inkijkje in de zaak van Ulbricht en alle gevolgen en media.



Tot de dag van vandaag blijven mensen ook twijfelen over de legitimiteit van de FBI haar handelingen en of het rechtsproces wel naar behoren is gegaan.