The Hague Centre
for Strategic Studies

HCSS Focus
Voor Clout en Cash

Gerben Bakker and Thijs van Aken

November 2026



The Hague Centre
for Strategic Studies

HCSS Focus
Voor Clout en Cash

November 2026

Auteurs
Gerben Bakker (Programmadirecteur Nationale Veiligheid en Weerbaarheid)
Thijs van Aken (Strategisch Analist)

Data-analyse en -visualisatie
Philippe van Pappelendam
Thijs van Aken (Strategisch Analist)
Sophie Tinselboer (Assistent Analist)

Redactie en review
Paul Sinning (CEO HCSS)

Projectleider Strategische Monitor Politie
Gerben Bakker (Programmadirecteur Nationale Veiligheid en Weerbaarheid)

Opdrachtgever
Directie Strategie en Innovatie, Staf Korpsleiding Nederlandse politie.

Met dank aan/met bijdragen van
Directie Strategie en Innovatie, Staf Korpsleiding Nederlandse politie.

Voor een goed begrip van de context en problematiek is voor deze verkenning gesproken met verschillende operationeel functionarissen bij de politie en in het veiligheidsveld.

Deze publicatie is **AI-supported**. De auteurs zijn volledig verantwoordelijk voor de integriteit van het werk. Zie de HCSS code of conduct for the responsible use of AI op HCSS.nl.

De analyses in dit rapport zijn afgerond in **september 2026**. Gebeurtenissen of ontwikkelingen die plaatsvonden in de periode tussen afronding en publicatie zijn niet van invloed geweest op de bevindingen.

© *The Hague* Centre for Strategic Studies behoudt zich alle rechten voor. Geen enkel onderdeel van dit rapport mag gere-produceerd of gepubliceerd worden in welke vorm dan ook, in print, microfilm, fotografie, of op enig andere manier zonder voorafgaande schriftelijke toestemming van HCSS. De rechten van alle foto's zijn voorbehouden aan hun respectievelijke eigenaars.

Omslagafbeelding: Canva (AI-gegenereerd)

Inhoudsopgave

Takeaways		**V**
1.	**Introductie**	**1**
1.1.	Een digitale ruimte zonder regie?	1
1.2.	Implicaties voor jongeren en maatschappij	2
1.3.	Het TikTok-platform als onderzoeksobject	6
2.	**Typen aangetroffen criminele content**	**8**
3.	**Snelweg naar criminele *content***	**13**
3.1.	Hoe het algoritme functioneert	13
3.2.	Blootstelling aan criminele content op TikTok	15
3.3.	Contentmoderatie op TikTok	20
4.	**Snelweg naar crimineel *handelen*?**	**23**
4.1.	Van open platform naar afgeschermd kanaal	23
4.2.	Strategische werving door criminele netwerken	25
5.	**Op zoek naar een antwoord**	**27**
5.1.	Vijf V's van de aanpak van digitale criminele content	27
5.2.	Knelpunten en strategische richtpunten	29
6.	**Conclusie**	**35**

Over de HCSS Focus

In deze HCSS Focus belichten we de snelheid van blootstelling aan criminele of criminaliteitsverheerlijkende content op TikTok. Daarbij speelt de veronderstelling dat consumptie van deze content kan bijdragen aan de normalisering van de criminele statuseconomie. Hierdoor ontstaat niet alleen een strafrechtelijk probleem maar ook een breder maatschappelijk risico waarbij jonge generaties mogelijk hun schouders sneller ophalen bij illegaal gedrag.

Een gerichte momentopname. Hoewel normalisering moeilijk te meten is, kunnen we initieel een probleem vaststellen in de enorm laagdrempelige toegang tot content. Deze HCSS Focus is gebaseerd op enkele kleinschalige OSINT-experimenten die HCSS uitvoerde aan de hand van TikTok-accounts. We hebben ons daarbij gericht op de snelheid waarmee schadelijke content op de tijdslijn verschijnt, welk type content verschijnt, en hoe effectief schadelijke content vervolgens weer verwijderd wordt na rapportage. Met de resultaten hebben we zo een impressie willen geven van de aard en omvang van het probleem van laagdrempelige en hardnekkige beschikbaarheid.

Strategisch belang voor beleid en debat. Het doel van deze Focus is primair om inzake de problematiek een signaal af te geven voor verder onderzoek en beleid. Bij wijze van eerste oriëntatie biedt deze verkenning ten slotte ook verscheidene sporen en richtingen voor de aanpak.

Takeaways

Het algoritme reikt de criminele statuseconomie actief aan

Steekproeven met enkele nieuwe TikTok-accounts illustreren dat gebruikers na enkele tientallen views al in aanraking kunnen komen met criminele content of content die verwijst naar een criminele status-economie.

Kijk naar de normalisering

De lage drempel tot dit soort content suggereert een sterke normaliserende werking: wie bedenkt dat honderdduizenden jongeren dagelijks dit soort content consumeren, begrijpt ook dat daarmee mogelijk een nieuw normaal gevestigd wordt. Op maatschappelijke schaal kan daar een ondermijnende werking vanuit gaan.

Contentmoderatie niet op orde

Van honderd gemelde posts die (naar ons oordeel) de regels van TikTok schonden, liet het platform er 81 ongemoeid. Moderatie verloopt grotendeels automatisch en mist mogelijk veel. Tussen 2023 en 2026 daalde het aantal Nederlandstalige moderatoren van 162 naar 45.

Van TikTok naar afgeschermde kanalen

Bijna de helft van de door ons aangemerkte accounts met criminele content (53 van de 119) verwees door naar andere kanalen zoals Snapchat of Telegram. Moderatie die alleen naar losse video's kijkt, mist die doorverwijzingsstructuur.

Leg de verantwoordelijkheid steviger bij het platform

Twee overkoepelende knelpunten lijken van terugkerende aard: een ontoereikende informatiepositie ten aanzien van snel veranderende digitale ecosystemen, en een asymmetrische machtsverhouding tussen overheden en internationale platformbedrijven. Aan kaders ontbreekt het niet zozeer, wel aan doorzettingsmacht. Platformen bepalen in hoge mate wat jongeren zien, maar worden daar nauwelijks op afgerekend. Er zijn meerdere concrete stappen te zetten om daaraan iets te doen.

1. Introductie

Deze HCSS Focus verkent de toegankelijkheid van criminele content op TikTok, de criminele contenttypen die daarbij te herkennen zijn, en de mogelijke route die dat soort content aanbiedt richting crimineel of illegaal gedrag. Daarnaast hebben we getoetst in hoeverre de door ons aangemerkte regel schendende content daadwerkelijk verwijderd wordt na melding. Deze verkenning is nadrukkelijk signalerend bedoeld. Ze geeft een indruk op basis van een beperkte steekproef van aangetroffen materiaal. Daarmee volstaan we in het aanstippen van de problematiek van hardnekkige, schadelijke content, maar benadrukken we ook dat dit onderzoek beperkt is in omvang, reikwijdte en diepgang. Dat laat onverlet dat de eenvoud waarmee dit soort content bereikbaar is tot maatschappelijke bezinning stemt over de normalisering van schadelijk materiaal online, en dat is dan ook de belangrijkste inzet van dit stuk.

Deze HCSS Focus is ontwikkeld in het kader van het programma **Strategische Monitor Politie (SMP)** dat HCSS uitvoert in opdracht van de Nederlandse politie. De SMP dient om toekomstgericht beleid te helpen ontwikkelen op het snijvlak van geopolitiek, maatschappelijke dynamiek en veiligheid. De HCSS Focus is hierin een strategisch duidend instrument en beoogt bij te dragen aan het beeld van veiligheidsprofessionals en een feitelijk debat. De analyse leent zich in die zin niet voor bindende empirische claims over hoe socialemediaplatformen zoals TikTok in de praktijk functioneren.

1.1. Een digitale ruimte zonder regie?

Er gaapt een steeds duidelijkere kloof tussen wat we in de fysieke wereld normaal vinden om tegen te komen en wat online dagelijks aan ons voorbijtrekt. Illegale, soms onmiskenbaar criminele content is op sociale media zonder noemenswaardige drempel te vinden. Dat lijkt eerder aan het aanbod te liggen dan aan de vraag. Om te beginnen circuleert er simpelweg veel dubieuze content. Deze komt, zo blijkt uit onze experimenten, vaak moeiteloos bovendrijven via de aanbevelingssystemen, zelfs bij nieuwe accounts zonder vooraf opgebouwd voorkeursprofiel.

Daar komt bij dat Nederland en Europa weinig grip hebben op socialemediabedrijven. Aan Europese ambities en regels geen gebrek, maar ze zijn niet altijd effectief. Handhavingspogingen zijn vaak niet opgewassen tegen de enorme hoeveelheid schadelijke content die rondgaat. Bovendien blijven Europese toezichthouders uiteindelijk afhankelijk van platformen die hun eigen richtlijnen hanteren, daarover weinig tot geen openheid van zaken geven en ook nog eens bezuinigen op hun eigen (Nederlandse) moderatiecapaciteit.[1] Tel daarbij op dat het aanbod vaak al inhoudelijk moeilijk te beheersen is, omdat beelden doorgaans veel verhullende of ambigue boodschappen bevatten die lang niet iedereen herkent. Ook moderatie-algoritmen hebben daar moeite mee.

[1] Vanmeldert, D. (2025, 2 augustus). TikTok ontslaat volledige moderatieteam in Berlijn, ook Nederlandstalige moderatoren getroffen. *VRT NWS*.

Gezien deze ontwikkelingen is de toenemende onrust over online grenzeloosheid begrijpelijk. Die zorgen gaan voor een belangrijk deel over de opgroeisituatie van de nieuwe internetgeneratie, voor wie confrontatie met dit soort content eerder de norm is dan de uitzondering. Deze verkenning wil vaststellen hoe snel een gebruiker met zulke content in aanraking kan komen. Hoe eenvoudiger dat gaat, hoe meer reden er ontstaat om socialemediaplatformen scherper te onderzoeken op hun bijdrage aan digitale normloosheid.

1.2. Implicaties voor jongeren en maatschappij

De zorgen over digitale normloosheid zijn niet nieuw, maar ze zijn de afgelopen jaren breder en concreter geworden. Op het criminele vlak zijn er grosso modo twee hoofdzorgen: 1) er zijn de zorgen over de verheerlijking en aanprijzing van een criminele, niets-ontziende levensstijl; 2) er zijn de steeds sterker aanwijsbare routes van socialemediagebruik naar daadwerkelijk crimineel gedrag. Samen vormen ze de context waartegen de bevindingen van deze studie moeten worden gelezen. Maar er zijn ook enkele kanttekeningen te plaatsen.

Normalisering van een criminele levensstijl. De eerste zorg raakt aan de vraag wat herhaalde blootstelling met jongeren doet. Er is een debat op gang gekomen over 'brain rot' en over afstomping (desensitisering) door herhaaldelijke confrontatie met schadelijke of gewelddadige content. Wie dagelijks beelden ziet van geweld, overvallen of stapels contant geld, raakt eraan gewend (zie kader onder). Daarnaast staan de verslavende effecten van schermgebruik steeds meer op het netvlies. De Europese Commissie concludeerde in februari 2026 voorlopig dat het ontwerp van TikTok, met eindeloos scrollen, pushmeldingen en een sterk gepersonaliseerd aanbevelingssysteem, in strijd is met de Digital Services Act. Volgens de Commissie brengen de voortdurende kleine beloningen gebruikers in een gedachteloze consumptiestand, wat compulsief scrollgedrag verder in de hand werkt (soms populair ook wel aangeduid als "doomscrollen").[2] Die combinatie maakt het probleem urgent, want ook content die criminaliteit normaliseert, komt binnen via een systeem dat erop is ingericht kijkers zo lang mogelijk vast te houden.

Clout en cash. De titel van deze HCSS Focus verwijst naar twee 'valuta' van de onlinestatuseconomie. *Clout* is digitale straattaal voor aanzien, invloed en reputatie, en wordt gemeten in views, likes, volgers en reacties. Criminologen Roks en Van den Broek onderzochten bijvoorbeeld hoe Rotterdamse drillrapjongeren online strijden om deze clout, waarbij provocaties en bedreigingen dienen om straatgeloofwaardigheid op te bouwen.[3] Socioloog Stuart liet zien hoe jongeren in Chicago hun online reputatie omzetten naar inkomsten.[4] Clout raakt daarmee aan het mechanisme van de aandachtseconomie. Het is de beloning waarop het verslavende ontwerp van platformen is ingericht: elke like is een kleine egobevestiging en een kans op succes.

Clout is in de digitale aandachtseconomie ook een bouwsteen van identiteit: wie online wordt gezien als rijk, succesvol of gevreesd, kan dat imagotechnisch bijschrijven. Criminele content

2 Europese Commissie. (2026a, 6 februari). *Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act* (persbericht).

3 Roks, R., & Van den Broek, J. (2020). *Cappen voor clout? Een verkennend onderzoek naar Rotterdamse jongeren, drill en geweld in het digitale tijdperk*. Erasmus Universiteit Rotterdam.

4 Stuart, F. (2020). *Ballad of the bullet: Gangs, drill music, and the power of online infamy*. Princeton University Press.

leent zich bij uitstek voor deze dynamiek, omdat geld en geweld aandacht trekken en het algoritme op zijn beurt deze aandacht beloont. Zo ontstaat een perverse cyclus waarin meer clout meer cash oplevert en vice versa, en waarin iedereen ook beelden helpt pushen die zoveel mogelijk sensatie en succes verbeelden. De Amerikaanse criminoloog Ray Surette spreekt in de context van criminele content in dit verband ook wel over "self surveillance" en "performance crimes": juist ook het crimineel gedrag wordt ostentatief. Het wordt expres vertoond met het oog op een publiek, waarbij de waardering van dat publiek het gedrag stimuleert.[5]

Criminologisch inzicht: hoe herhaalde blootstelling een normaliserende werking kan hebben. Criminologen als Sutherland en Akers hebben gesteld dat crimineel gedrag (ten dele) wordt aangeleerd via de attitudes, motieven en rechtvaardigingen die een persoon oppikt in zijn sociale omgeving. Frequentie, duur en jonge leeftijd zijn daarbij bepalend. Hoewel de fysieke sociale omgeving daarbij altijd als uitgangspunt diende, hoeven die rolmodellen zich niet in de directe sociale omgeving van het individu te bevinden. Nu sociale media en online influencers de belevingswereld van jongeren in belangrijke mate bepalen, is het aannemelijk dat ook daarvan een socialiserende werking uitgaat. Criminele content en het ethos van succes, geld en dominantie leveren dan een doorlopende stroom van rolmodellen en rechtvaardigingen voor normoverschrijdend en crimineel gedrag. Recent onderzoek beschrijft influencers in dit verband zelfs als digitale 'superpeers': leeftijdsgenoten op afstand wier opvattingen jongeren serieus nemen.[6]

Routes naar crimineel gedrag. Als het gaat om de weg van socialemediagebruik naar daadwerkelijk crimineel gedrag, kan men een passieve en een directe route onderscheiden. De passieve route berust op hiervoor besproken digitaal-culturele beïnvloeding, en gaat ervanuit dat consumptie van criminaliteitsverheerlijkende content uiteindelijk ook de drempel verlaagt om sneller iets illegaals te doen. Dat verband is moeilijk hard te maken, omdat de causale relaties tussen beeldconsumptie en de omarming van crimineel gedrag niet te isoleren zijn. Dat betekent echter niet dat het verband afwezig is.

Bij de directe route worden jongeren via sociale media rechtstreeks benaderd voor criminele activiteiten. Hier zijn wel veel duidelijker aanwijzingen voor omdat het gaat om expliciete oproepen waar soms op wordt gereageerd. Onderzoek voor het programma Politie en Wetenschap onder ruim duizend jongeren van 16 tot 27 jaar wees bijvoorbeeld uit dat één op de vijf op sociale media weleens een oproep voor drugs- of geweldsdelicten heeft gezien. Ruim zes procent werd daarbij zelf benaderd, vooral via Snapchat en TikTok. De oproepen zijn meestal vaag geformuleerd, maar soms wordt openlijk geworven, zelfs voor liquidaties.[7] Criminele netwerken gebruiken socialemediaplatformen dus inmiddels expliciet als wervingskanaal en als digitale marktplaats waar klussen worden aangeboden en afnemers worden gezocht.

---

5 University of Central Florida. (z.d.). *A culture of self-surveillance: Social media and crime*; Surette, R. (2016). How social media is changing the way people commit crimes and police fight them.

6 Bronnen: Sutherland, E. H. (1947). *Principles of criminology* (4e druk). Lippincott; Akers, R. L. (1998). *Social learning and social structure: A general theory of crime and deviance*. Northeastern University Press; Van Houtven, W., & Schmuck, D. (2026). Influencers perceived as digital super peers? Outcomes of adolescents' use of social media influencers for socio-political information. *Journal of Computer-Mediated Communication*, 31(2).

7 Bergers, J., Van Deuren, S., Roks, R., Habets, S., Leukfeldt, E. R., & Eichelsheim, V. I. (2026). *De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit* (Politiekunde 133). Politie en Wetenschap.

Beide routes hangen uiteindelijk samen met de infrastructuur van de platformen en hun aanbevelingssystemen. Die bepalen voor een groot deel wat jongeren in hun tijdlijn te zien krijgen, en in hoeverre criminele content en geweldsverheerlijkende beelden kunnen meeliften op al het andere wat wordt aangeboden. Waar de aandacht lange tijd vooral uitging naar het dark web als marktplaats voor criminele handel en dienstverlening, is die daarom nu terecht (deels) verschoven naar de grote, reguliere platformen, waar jongeren toch al een groot deel van hun tijd doorbrengen. Als de drempel naar criminaliteit inderdaad wordt verlaagd door de manier waarop platformen zijn ingericht, is het uiteraard legitiem om juist de werking van deze infrastructuur kritisch te bekijken.

Bredere maatschappelijke effecten. Op de langere termijn en vanuit een overkoepelend gezichtspunt overstijgen de maatschappelijke zorgen het particuliere en acute probleem van jongeren die, eventueel op basis van extra digitale stimulans, in de criminaliteit belanden. Sommige onderzoekers signaleren eerder generationele problemen in de identiteitsvorming van met name jonge mannen. Kijkend naar de criminele levensstijl verschijnen er ook dwarsverbanden naar de manosphere en naar een bredere internetcultuur waarin de mannelijke zelfhulplogica regeert geënt op een recht-van-de-sterkste-mentaliteit en de verheerlijking van het (digitaal) pooierschap.

Een voorbeeld is superfluencer Andrew Tate, die inmiddels herhaaldelijk is gearresteerd. Zijn programma's, zoals 'Hustler's University' en 'The War Room', combineren het opzetten van dubieuze verdienmodellen met zelfontwikkeling op basis van een ultraconservatief en gewelddadig manbeeld. Ze telden honderdduizenden leden, en video's van Tate werden op TikTok miljarden keren bekeken.[8] Het laat zien hoe (quasi-)criminele content vervloeit met andere digitale subculturen die inspelen op beelden van financieel en seksueel succes. Op de achtergrond bestaat zo een veel breder digitaal ecosysteem dat een crimineel pad min of meer stilzwijgend presenteert als logische keuze voor wie voor zichzelf opkomt. De aantrekkingskracht daarvan berust niet alleen op de algoritmische fuik waarin jongeren terechtkomen, maar ook op de schijnbaar eenvoudige oplossingen die deze narratieven bieden voor de problemen, onzekerheden en angsten waarmee vooral kansarme jongeren kunnen worstelen.[9] Wat criminele content aantrekkelijk maakt, is dus behalve de belofte van geld en status ook het twijfelachtige, maar bereikbare ethos en de identiteit die ze aanreikt.

Het effect van deze 'hustle culture' reikt verder dan de groep die uiteindelijk in de criminaliteit terechtkomt. Naarmate het ethos breder wordt gedeeld, verschuift het normenkader van een hele generatie, zo is de angst, en ontstaat mogelijk een voedingsbodem voor uiteenlopende ondermijnende narratieven. De normaliserende werking van criminele content op TikTok kan zo het 'sociale sneeuwbaleffect' versterken waarmee jongeren ook sneller kunnen ingroeien in de georganiseerde criminaliteit, zeker als deze fysieke sociale netwerken er al liggen. Naast mechanismen als bewuste rekrutering en de invloed van werk, hobby's en ingrijpende levensgebeurtenissen bewegen sommige jongeren zo eenvoudiger mee met een sociale omgeving waarin criminaliteit steeds gewoner wordt en tegelijkertijd resoneert met de leefstijl die ze online zien.[10] Een algoritmisch gevoede, geld- en geweldsverheerlijkende contentomgeving vergroot de sociale omgevingsfactor. Niet alleen buurt- en klasgenoten fungeren dan als voorbeeld van 'normaal' succes, maar ook duizenden anonieme accounts.

---

8 Magee, C. (2023, 27 januari). I went inside Andrew Tate's Hustler University – where 'Gs' celebrate making $11. *The Independent*; Das, S. (2022, 6 augustus). Inside the violent, misogynistic world of TikTok's new star, Andrew Tate. *The Guardian*; Associated Press. (2022, 30 december). Andrew Tate, the divisive social media star, detained in Romania. *Associated Press*; Associated Press. (2024, 12 maart). Online influencer Andrew Tate detained in Romania, handed U.K. arrest warrant, his spokesperson says. *NBC News*.

9 Flood, M., & Keddie, A. (2026). Inspiration, advocate, hypocrite or predator? Young men's diverse views of Andrew Tate. *Gender and Education, 38*(6), 598–615.

10 De Boer, H., Ferwerda, H., & Kuppens, J. (2022). *Do or don't: Kennissynthese ingroeimechanismen en rekruteringsprocessen van jongeren in de georganiseerde criminaliteit*. WODC.

Op macroniveau worden deze effecten niet noodzakelijk onomstotelijk bewezen maar wel waargenomen. Europol wees er eerder op dat de uitbuiting van jonge daders het sociale weefsel van de samenleving beschadigt en tegelijk de bovenlaag van criminele netwerken buiten beeld houdt.[11] Die dynamieken versterken elkaar. Naarmate meer jongeren beschikbaar zijn als uitvoerder, blijft de bovenlaag verder buiten bereik van opsporing, en naarmate die laag onaantastbaar blijkt, wint het criminele verdienmodel aan geloofwaardigheid als voorbeeld van succes.

Deze verkenning is uiteindelijk niet diepgaand genoeg om vast te stellen in welke mate sociale media precies van invloed zijn op de rekrutering van jongeren in de georganiseerde misdaad, noch welke macro-effecten van normalisering van criminele stijlen aangetoond kunnen worden. Wel laat ze zien hoe normvervagende en criminaliteitsverheerlijkende content ten minste zeer eenvoudig te bereiken is, waarmee een gezichtspunt ontstaat op de eerste stap van dit probleem.

Relativering. Tegen de zojuist besproken zorgen en geopperde verbanden kunnen ook zaken worden ingebracht. Zo kan worden benadrukt dat content op sociale media misschien 'maar' virtueel, vluchtig en vrijblijvend is, en dat jongeren mogelijk minder gevoelig zijn voor wat er op hun tijdlijn voorbijkomt dan vaak wordt aangenomen. Dat bezwaar veronderstelt een relatief gescheiden beleving van de online en offline leefwereld. De cijfers over internetconsumptie ondersteunen dat beeld niet direct, ook al zegt dat niet alles. In 2025 was 96 procent van de Nederlandse bevolking van 12 jaar of ouder dagelijks online, en was 93 procent van de 12- tot 25-jarigen actief op sociale netwerken.[12] Dat benadrukt in ieder geval de forse tijdsinvestering online.[13] Volgens het Nationaal Social Media Onderzoek 2025 besteden Nederlanders gemiddeld bijna twee uur per dag aan sociale media. Onder jongeren van 15 tot 19 jaar bedraagt dit zelfs gemiddeld 2 uur en 45 minuten per dag.[14] Posts die jongeren tegenkomen, zijn soms afkomstig van personen die zowel offline als online als rolmodel fungeren, wat suggereert dat hun invloed ook digitaal behoorlijk kan doorwerken.

Tegelijk is een verband tussen sociale media en criminaliteit niet automatisch oorzakelijk. Jongeren die al crimineel actief zijn, of in omgevingen verkeren waarin veel social peers crimineel gedrag laten zien, zoeken zulk gedrag makkelijker op, en belanden mogelijk eerder in digitale bubbels waarin criminaliteit de norm is. Sommige criminologen wijzen er zelfs op dat de opkomst van sociale media en smartphones heeft bijgedragen aan de daling van de jeugdcriminaliteit sinds 2010.[15] Bergers e.a., de onderzoekers achter het voornoemde onderzoek voor Politie en Wetenschap wijzen erop dat termen als 'ronselen' en 'rekrutering' dwang suggereren, terwijl een deel van de jongeren zich bewust en op eigen initiatief aanbiedt voor een criminele klus.[16] Dit suggereert dat er bij een deel van de jongeren voldoende motivatie is opgebouwd om zelf naar snel geld te zoeken. Kortom, er zijn ook redenen om het medium minder als aanstichter te zien van criminele tendensen en te wijzen op criminogene patronen die altijd al bestonden.

---

11 Europol. (2025). *The changing DNA of serious and organised crime: European Union serious and organised crime threat assessment 2025*. Europol, p. 89.

12 Centraal Bureau voor de Statistiek (CBS). (2026a). *Digitalisering en kenniseconomie 2025*. CBS. Gebaseerd op StatLine-tabel 84888NED, *Internettoegang en internetactiviteiten; persoonskenmerken*.

13 Hoeben, E., Weerman, F., & Weulen Kranenbarg, M. (2024). *Leiden sociale media tot meer jeugdcriminaliteit?* (factsheet). Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.

14 Van der Veer, N., Bloemert, E., & Lohuis, J. (2025). Nationale Social Media onderzoek 2025. Newcom Research & Consultancy.

15 Hoeben, E., Weerman, F., & Weulen Kranenbarg, M. (2024). *Leiden sociale media tot meer jeugdcriminaliteit?* (factsheet). Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.

16 Bergers, J., Van Deuren, S., Roks, R., Habets, S., Leukfeldt, E. R., & Eichelsheim, V. I. (2026). *De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit* (Politiekunde 133). Politie en Wetenschap.

Toch, wanneer leven, werken en socialiseren meer en meer digitaal verlopen, gaat wat op deze platformen circuleert onvermijdelijk deel uitmaken van het normatieve repertoire. Maar omdat normaliserende effecten in essentie moeilijk te meten zijn, blijft dit aspect snel een blinde vlek in het denken over de bronnen van criminaliteit en ondermijning. Wanneer blootstelling een generatie voortbrengt die haar schouders ophaalt over hoe geld wordt verdiend en haar identiteit verknoopt aan criminele statussymbolen, ontstaat een voedingsbodem voor ondermijning die nog lang kan doorwerken.

1.3. Het TikTok-platform als onderzoeksobject

Deze HCSS Focus is nadrukkelijk verkennend van opzet. Het doel is niet de omvang van criminele content op sociale media vast te stellen, maar hooguit inzichtelijk te maken hoe snel en langs welke routes gebruikers ermee in aanraking kunnen komen. Daarvoor is gekozen voor één platform, TikTok, dat om meerdere redenen een logisch onderzoeksobject is voor de Nederlandse situatie:

- *Gebruiksintensiteit.* Jongeren brengen veel tijd door op TikTok. Het platform is daarmee een vast onderdeel van hun dagelijkse leefwereld.
- *Aansluiting bij eerder onderzoek.* O.a. het onderzoek van Bergers e.a. wijst TikTok, naast Snapchat, aan als een van de platformen waarop jongeren het vaakst worden benaderd voor drugs- of geweldsdelicten.[17]
- *Europees toezicht.* TikTok staat als zeer groot onlineplatform onder direct toezicht van de Europese Commissie. Die voert sinds februari 2024 een formele procedure naar onder meer de bescherming van minderjarigen en het verslavende ontwerp van de app, en kwam in 2026 op beide punten met voorlopige bevindingen.[18] Een toetsende verkenning van de content en de moderatie ervan sluit daarop aan.
- *Een aanbevelingsplatform in zuivere vorm.* Snapchat draait vooral om onderlinge communicatie tussen bekenden, en Instagram combineert een sociaal netwerk met een aanbevelingsfeed. Op TikTok is de algoritmische For You-feed het hart van de app. Het mechanisme waar deze studie om draait, het ongevraagd aanreiken van content, is daar het duidelijkst zichtbaar.

Hoe dat uitpakt, laat het OSINT-onderzoek voor deze studie zien. De For You-pagina presenteerde de criminele levensstijl als een van de routes naar succes en geld. Het algoritme bood daarbij verschillende criminele contentmilieus aan voor verschillende soorten gebruikers, van cryptofraude en money schemes tot het verheerlijken van geweld en het aanbieden van drugs. De normalisering van een criminele levensstijl beperkt zich niet tot één doelgroep van vooraf geprofileerde belangstellenden, maar bereikt direct al een breed en gevarieerd publiek.

Omdat deze studie zich concentreert op de toegankelijkheid en prevalentie ligt de nadruk niet op besloten berichtenverkeer. Juist voor dat publieke aanbod is TikTok zeer relevant. Voor platformen als Instagram of Telegram geldt dat in mindere mate, omdat de communicatie van

---

17 Bergers, J., Van Deuren, S., Roks, R., Habets, S., Leukfeldt, E. R., & Eichelsheim, V. I. (2026). *De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit* (Politiekunde 133). Politie en Wetenschap.

18 Europese Commissie. (2026d, 24 juli). *Commission preliminary finds TikTok in breach of Digital Services Act for failing to ensure safe accounts for minors* (persbericht); Europese Commissie. (2026a, 6 februari). *Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act* (persbericht).

persoon tot persoon sneller centraal staat of de mate van openbaarheid anders ligt. Tot slot draagt het type 'short form' content bij aan de keuze voor TikTok. Het korte videoformat is ontworpen voor snelle consumptie, oppervlakkige steun, verspreiding en imitatie.

Onderzoeksmethode en totstandkoming. De onderzoeksresultaten van deze HCSS Focus zijn tot stand gekomen op basis van eigen verkenningen op TikTok, aangevuld met bestaande inzichten over online werving door criminele netwerken. Het onderzoek beperkt zich tot openbare kanalen; er is geen direct contact geweest met andere gebruikers. Het is signalerend van aard en niet representatief voor elke gebruikerservaring. Omdat het een fenomeenanalyse betreft, wordt niet ingegaan op individuele accounts of gebruikers. De aanpak bestond uit vijf stappen.

- **Stap 1: verkenning en escalatieladder.** Een verkenning van overwegend Nederlandstalige TikTok-content leverde de vijf contenttypen op die in hoofdstuk 2 worden beschreven. Daarnaast is een escalatieladder ontwikkeld met vijf niveaus, van neutrale content tot expliciete criminaliteit en diensten (Tabel 1). Met die ladder is in de experimenten elke video gescoord.
- **Stap 2: steekproef met een nieuw account.** Met een nieuw account zonder voorgeschiedenis zijn de eerste duizend aanbevolen video's bekeken en gescoord. Video's met relevante content zijn volledig uitgekeken en geliket, zoals een geïnteresseerde gebruiker zou doen (paragraaf 3.2).
- **Stap 3: steekproef met gesimuleerde interesses.** Vijf nieuwe accounts bootsten elk een andere, niet-criminele interesse na, zoals ondernemerschap, politieoptreden en straatcultuur. Per thema zijn in twee sessies 130 video's bekeken en op dezelfde wijze gescoord.
- **Stap 4: doorverwijzingssteekproef.** Van 119 accounts met criminaliteitsverheerlijkende of expliciet criminele content is nagegaan of en hoe zij gebruikers doorverwijzen naar andere platformen, zoals Telegram en Snapchat (hoofdstuk 4).
- **Stap 5: moderatiesteekproef.** Honderd posts die naar ons oordeel de Community Guidelines van TikTok schenden, zijn via de meldfunctie gerapporteerd, waarna is bijgehouden hoe TikTok de meldingen afhandelde (paragraaf 3.3).

Leeswijzer. Dit rapport is opgebouwd van duiding naar strategische oriëntatie. Hoofdstuk 1 schetst de context en de maatschappelijke urgentie. Hoofdstuk 2 brengt in kaart welke typen malafide content aangetroffen is in de steekproeven. Hoofdstuk 3 laat aan de hand van de steekproeven zien hoe snel het aanbevelingsalgoritme nieuwe gebruikers naar die content leidt, en hoe TikTok omgaat met meldingen ervan. Hoofdstuk 4 belicht de doorverwijzingsstructuur. Hoofdstuk 5 benoemt waarom de aanpak in de praktijk weerbarstig verloopt en formuleert richtpunten voor beleid.

2. Typen aangetroffen criminele content

Veel van wat op TikTok rondgaat, is inhoudelijk onschuldig. Toch wordt het platform ook gebruikt om een criminele levensstijl te etaleren, illegale diensten aan te prijzen en jongeren te benaderen voor klussen. Hoe groot dat aandeel is, is moeilijk vast te stellen. TikTok publiceert wel hoeveel video's het verwijdert, maar niet hoeveel schadelijke content de moderatie passeert. Daar komt bij dat veel content in een grijs gebied valt. Een video met stapels contant geld is op zichzelf niet illegaal, maar kan wel een criminele levensstijl aanprijzen.

Vijf contenttypen. Op basis van onze verkenning van overwegend Nederlandstalige TikTok-content zijn vijf contenttypen te onderscheiden. Het onderscheid is gebaseerd op de functie die de content vervult. In de praktijk lopen de typen in elkaar over. Ook willen we niet suggereren dat het hier gaat om een sluitende typologie. De typen zijn aangevat ter structurering en komen in hoofdstuk 3 terug in de manier waarop de contentanalyse verder werd verdiept.

Crimineel bijverdienen

In dit type content wordt criminaliteit gepresenteerd als een snelle en toegankelijke manier om geld te verdienen. Naar de illegale kant wordt meestal alleen impliciet verwezen. Europol beschrijft hoe wervende berichten daarbij de taal van legaal werk overnemen, met termen als 'job opportunity' en 'business', waardoor het criminele karakter naar de achtergrond verdwijnt.[19] Nederlands onderzoek laat een vergelijkbaar patroon zien. Het eerste contact begint doorgaans met een vage oproep voor 'werk' of een 'klus', zonder dat duidelijk is waar het om gaat.[20] Die vaagheid verlaagt de drempel om te reageren, omdat een reactie nog nergens toe verplicht. Wat de klus inhoudt, wordt soms pas later duidelijk, in een privéchat of op een ander platform (zie hoofdstuk 4). In onze verkenning kwamen regelmatig posts voor die verwezen naar illegale handeltjes, zoals de verkoop van nepgeld, illegale vapes, signaalblokkers en inbraakgereedschap (zie paragraaf 3.2). Niet elke post die een crimineel verdienmodel toont, blijkt een serieus aanbod. Soms dient een bericht vooral om status uit te stralen.

19 Europol. (2024). *The recruitment of young perpetrators for criminal networks* (intelligence notification). Europol.

20 Bergers, J., Van Deuren, S., Roks, R., Habets, S., Leukfeldt, E. R., & Eichelsheim, V. I. (2026). *De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit* (Politiekunde 133). Politie en Wetenschap.

Verheerlijken criminele lifestyle

De hang naar een luxe levensstijl uit zich in zeer veel beschikbare video's waarin criminele statussymbolen worden getoond zoals stapels geld, horloges, auto's enz. Contentmakers etaleren soms spullen die (schijnbaar) gestolen of geheeld zijn. Maar lang niet alles is per definitie echt. Een deel van het getoonde geld op TikTok is zogeheten prop money, filmgeld dat rijkdom moet suggereren zonder dat er een criminele bron achter zit. Ook in onze experimenten werd regelmatig met nepgeld gepronkt. Dit soort content zegt daarom nog weinig over de daadwerkelijke criminele betrokkenheid van de maker. Vaker gaat het om lifestyle signalling, het opbouwen van status en geloofwaardigheid door crimineel succes te suggereren.

Fraude en "money schemes"

Binnen het bijverdiengenre is er de nichecontent van fraudemodellen, waaronder ook de aangeboden "money schemes" of "money flipping-content" vallen. Daarin worden allerlei trucs aangeboden om de inleg van betrokkenen te verdubbelen of te verdrievoudigen, vaak via schimmige cryptovalutaroutes. Er moet vaak worden betaald via prepaidkaarten of betaalapps, waarna het geld verdwijnt.[21] Een andere variant zijn zogeheten "hustle-guru's" die cursuspakketten en toegang tot besloten groepen aanbieden waarin methoden worden gedeeld om snel rijk te worden. Zulke constructies presenteren deelname als een vorm van slim ondernemen. In de praktijk brengen ze deelnemers met name in de problemen omdat het gaat om een (verkapt) piramidespel of om illegale activiteiten. "Refund schemes" zijn weer een ander fenomeen. Gebruikers kunnen tegen betaling toegang krijgen tot verschillende oplichtingsmethoden, bijvoorbeeld door te liegen over de aankomst of inhoud van een pakket, of door het verwisselen van de inhoud in een retourpakket.[22]

Spot drijven met politie en gezag

Hoewel het niet gaat om expliciete criminele gedragsaanprijzingen of verdienmodellen zijn er ook veel video's te vinden waarin de politie of andere gezagsdragers worden bespot of geprovoceerd. Nederlandse voorbeelden tonen jongeren die agenten of BOA's op straat uitdagen of eventueel zelfs aanvallen, op jacht naar clout. In de feed verschijnen regelmatig (mislukte) politieachtervolgingen. In een enkel geval verschenen ook gevallen van vandalisme van politie-eigendommen. Een verwante categorie is provocatieve content van gedetineerden welke laat zien hoe makkelijk ze allerlei voorwerpen naar binnen kunnen smokkelen, bijvoorbeeld met drones of andere constructies. Soms tonen video's schijnbaar het 'casual' dagelijks leven in de gevangenis.[23] Zulke video's tonen vooral dat het gezag geen greep heeft op de maker. De Nederlandse politie is inmiddels zelf op TikTok actief, met speciaal daarvoor geselecteerde agenten.

---

21 CommunityAmerica Credit Union. (2024). *Money flipping fraud*.

22 Tullen, S. (2026, 12 augustus). *I joined a refund scamming community* (video). YouTube.

23 BRUZZ. (z.d.). Ondanks strikt verbod op gsm's: TikTok-account toont 'dagelijks leven' in gevangenis Haren.

Uitingen van straatcultuur en drillrap

Ten slotte, een deel van de openbare content op TikTok kan worden opgevat als een uiting van gewelddadige straatcultuur waarin groepsloyaliteit en rivaliteit centraal staan. Het gaat om video's waarin jongeren hun wijk en vriendengroep neerzetten als "hun" territorium, en confrontaties, achtervolgingen, bedreigingen of vechtpartijen delen als bewijs van status.

Een van de meer specifieke contentvormen is drillrapmateriaal. Op TikTok verschijnt drillrap vooral in de vorm van korte edits, onder rapmuziek gezet, waarin bijvoorbeeld rivaliserende groepen worden geïntimideerd of bedreigd. Content kan ook de vorm hebben van opgenomen confrontaties dan wel steekpartijen tussen personen die elkaar hebben uitgedaagd. Het is bekend dat ook in Nederland drillrapgroepen actief zijn en dat er geweldsincidenten voorkomen, met name in de regio Rotterdam. [24]

[24] Roks, R., & Van den Broek, J. (2020). *Cappen voor clout? Een verkennend onderzoek naar Rotterdamse jongeren, drill en geweld in het digitale tijdperk*. Erasmus Universiteit Rotterdam.

Criminele contenttypen op TikTok

Normaliserende content en expliciete criminaliteit



Crimineel bijverdienen

Video's prijzen expliciet en impliciet criminele activiteiten aan als een snelle manier om veel geld te verdienen. Dit gaat gepaard met vertoon van geld en dure goederen, vage oproepen voor 'werk' en het vertoon van illegale goederen.



Verheerlijken criminele lifestyle

Video's etaleren geld en luxe als een bewijs van crimineel succes. Makers pronken met stapels contant geld, sieraden, designerkleding en dure auto's, en soms met gestolen spullen. Goederen zijn niet altijd echt, maar geven hetzelfde signaal af.



Fraude en money schemes

Video's presenteren dubieuze manieren om snel rijk te worden als ondernemerschap. Denk aan fraude, money flipping en cryptoscams. Gebruikers verkopen handleidingen of workshops waarin ze deze methodes uitleggen.



Spot drijven met politie en gezag

Video's framen de politie negatief, drijven de spot met agenten of verheerlijken het ontlopen van een aanhouding. Bijvoorbeeld met provocaties op straat, vandalisme en vlogs van gedetineerden die hun veroordeling romantiseren.



Uitingen van straatcultuur en drillrap

Video's laten confrontaties, achtervolgingen en vechtpartijen zien als bewijs van status. Drillrapfragmenten met gemaskerde gezichten en provocaties richting andere groepen versterken dat beeld.

Bron: OSINT-onderzoek | Steekproef

Reflectie op ambiguïteit en strafbaarheid

De vijf contenttypen verschillen weliswaar in vorm en boodschap, maar ze vertonen wel gemeenschappelijke motieven. Bijvoorbeeld, ze bewegen zich regelmatig net buiten het bereik van het strafrecht. Daarbij is vaak sprake van een semantisch spel tussen opsporing en content creators: men ontwikkelt allerlei 'algospeak' of dubbelzinnigheden (bij digitaal extremisme wordt in dat geval ook wel over 'borderline content' gesproken) die duidelijk maken bij de ontvanger waarover de boodschap gaat maar die minder makkelijk herkend kunnen worden als verwijzend naar iets strafbaars of illegaals.

In meerdere geanalyseerde TikToks wordt dit soort alternatieve termen gebruikt. Zo wordt de synthetische drug Spice aangeboden als "haarolie" of "showergel", wordt inbraakgereedschap verkocht "voor als je je sleutels kwijt bent" en wordt een oproep voor een criminele klus verpakt als een "vacature". Dit gebruik van gecodeerde woorden, emojis of symbolen is ook geschikt om geautomatiseerde moderatie te omzeilen. Europol signaleert eenzelfde patroon bij de rekrutering van jongeren via sociale media: makers vervangen drugsgerelateerde termen door alledaagse woorden of symbolen.[25] Soms is het aangeboden product op zichzelf legaal en wordt het pas verdacht door de context waarin het wordt aangeprezen, zoals bij lockpicksets of objecten met verborgen bergruimtes. En soms is simpelweg niet vast te stellen of wat in beeld komt echt is. Stapels geld kunnen filmgeld zijn, een vuurwapen kan een replica zijn, en een gefilmde overval kan nieuwsmateriaal zijn dat als meme wordt hergebruikt. Wie thuis in een video met een keukenmes zwaait op een drillrapbeat, zonder daarbij iemand concreet te bedreigen, doet in de regel nog niets strafbaars.

Of deze dubbelzinnigheid steeds bewust wordt gezocht, is uiteraard hoogst aannemelijk, maar de mate waarin valt op basis van dit onderzoek niet met zekerheid te zeggen. Ook weegt mee dat een deel van de contentmakers gemotiveerd is door primair stoerdoenerij dan door oprechte criminele motieven en communicatie. Voor de totale normaliserende werking van content doen de achterliggende motieven minder ter zake. Of stapels geld echt zijn, of een wapen geladen is of niet, de onderliggende verheerlijkende boodschap blijft problematisch.

Content die niet aantoonbaar strafbaar is, valt uiteraard buiten het bereik van politie en justitie, terwijl ze mogelijk wel de huisregels van het platform schendt. Dat legt de verantwoordelijkheid voor een groot deel van dit aanbod nog weer extra bij de moderatie van het platform zelf, maar juist daar blijkt deze dubbelzinnigheid het moeilijkst te herkennen (zie paragraaf 3.3). Zeker ook als platformmoderatie niet geschiedt in relatie met het Nederlands taalgebied.

[25] Steen, E., Yurechko, K., & Klug, D. (2023). You can (not) say what you want: Using algospeak to contest and evade algorithmic content moderation on TikTok. Social Media + Society, 9(3); Europol. (2024). *The recruitment of young perpetrators for criminal networks* (intelligence notification). Europol.

3. Snelweg naar criminele *content*

Het bestaan van deze contentmilieus zegt nog niks over hoe jongeren hiermee in aanraking kunnen komen. Die route loopt niet enkel via gerichte zoekopdrachten, maar via aanbevelingen die TikTok ongevraagd doet. Dit hoofdstuk illustreert aan de hand van OSINT-onderzoek hoe de weg ten dele naar criminele content voert.

3.1. Hoe het algoritme functioneert

Het TikTok-algoritme is ontworpen om de interesses van gebruikers te identificeren en het aanbod van video's daarop af te stemmen. De For You-pagina selecteert deze video's op basis van het gedrag van de gebruiker, zoals kijktijd, herhaald bekijken, likes, shares, reacties en zoekgedrag. Om video's voor te stellen die opnieuw tot veel interactie zullen leiden, combineert het systeem deze signalen met de specifieke kenmerken van een video, zoals geluid, hashtags en bijschrift.[26] Bij nieuwe accounts stelt het systeem eerst algemene, virale video's voor om te observeren hoe een gebruiker daarop reageert, om op basis daarvan het aanbod verder toe te spitsen. Een analyse van de kijkgeschiedenis van 220 gebruikers toont dat van de eerste duizend voorgestelde video's, 30 tot 50 procent is toegespitst op de interesses van de gebruiker.[27] Al binnen de eerste 200 bekeken video's begint het algoritme met het voorstellen van video's die zijn afgestemd op het opgebouwde profiel van de gebruiker.[28]

De verslavende werking van het algoritme. Zoals bekend staat dit type technische ontwerp in dienst van het verdienmodel van het platform: hoe beter het consumptiegedrag in beeld is en het kijkgedrag te sturen, hoe beter advertenties te targeten zijn. Het algoritme is dan ook zo ingericht dat het steeds kleine beloningen afgeeft die aanzetten tot doorkijken.[29] Dit mechanisme wordt vaak in verband gebracht met een verslavende dopaminecyclus (zie onderstaande figuur). Wanneer de hersenen een beloning registreren, bijvoorbeeld een prikkelende video, komt dopamine vrij en ervaart de gebruiker een drang naar meer. TikTok en andere sociale media spelen op dit mechanisme in door met een continue stroom aan gepersonaliseerde content telkens opnieuw dopamine-afgifte uit te lokken. Doordat het lichaam aan deze constante stimulus went, ontstaat het verlangen naar steeds langer gebruik en meer interactie.[30]

---

26 TikTok. (z.d.). *Introduction to the TikTok recommendation system*; Boeker, M., & Urman, A. (2022). An empirical investigation of personalization factors on TikTok. In *Proceedings of the ACM Web Conference 2022* (pp. 2298–2309). ACM.

27 Vombatkere, K., et al. (2024). TikTok and the art of personalization: Investigating exploration and exploitation on social media feeds. In *Proceedings of the ACM Web Conference 2024* (pp. 2789–2797). ACM.

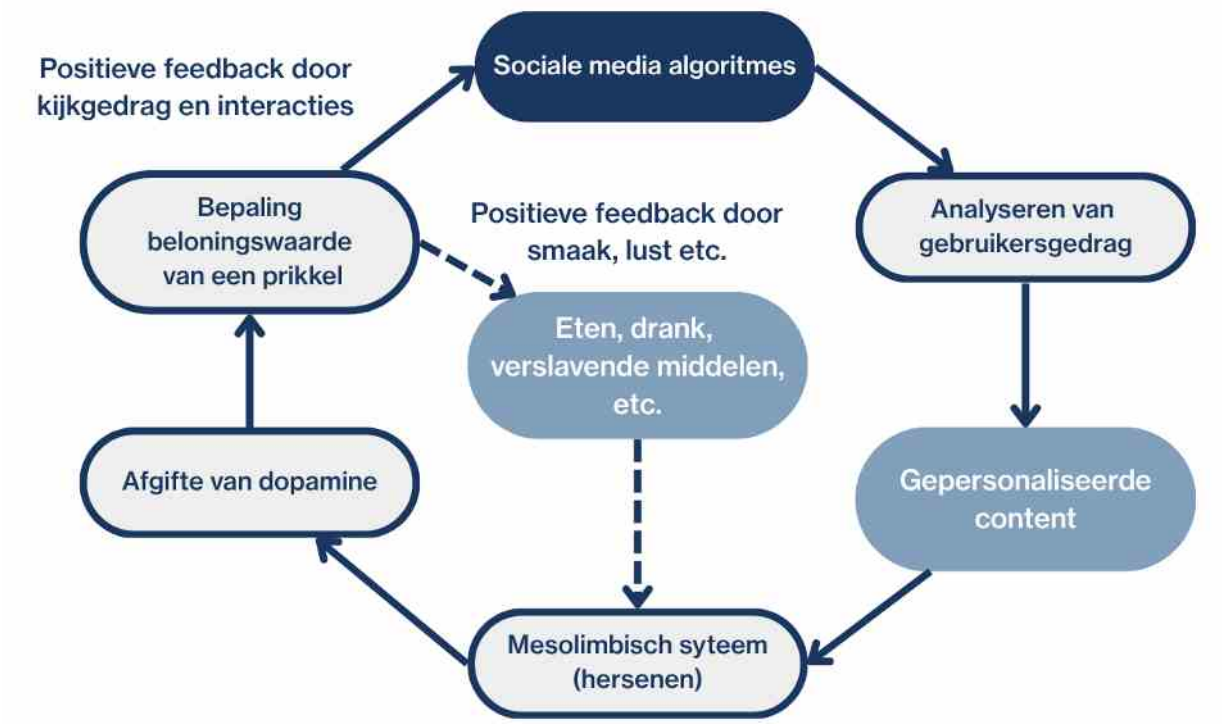
28 Baumann, F., et al. (2026). Dynamics of algorithmic content amplification on TikTok. *EPJ Data Science, 15*, 18.

29 Negreiro, M., & Anaç, Ö. D. (2026). *Addictive design on online platforms*. European Parliamentary Research Service.

30 De, D., et al. (2025). Social media algorithms and teen addiction: Neurophysiological impact and ethical considerations. *Cureus, 17*(1), e77145.

Jongeren zijn hiervoor extra kwetsbaar. In de tienerjaren is het beloningssysteem in de hersenen al volop ontwikkeld, terwijl het gebied dat impulsen afremt pas rond 25-jarige leeftijd is volgroeid.[31] Deze kwetsbaarheid komt ook naar voren in cijfers van de WHO. Elf procent van 280.000 ondervraagde jongeren (11, 13 en 15 jaar) in 44 landen vertoonde problematisch socialemediagebruik: ze konden niet stoppen en ondervonden daarvan negatieve gevolgen. In Nederland lag dit percentage op 5 procent.[32]

Figuur 1. Verslavende werking van het algoritme



Geadapteerd van: De, D., et al. (2025). Social Media Algorithms and Teen Addiction: Neurophysiological Impact and Ethical Considerations. Cureus, 17(1), e77145.

De weg naar extreme en gewelddadige content. Dat dit aanbevelingssysteem gebruikers niet alleen tot onschuldige niches drijft, is breed gedocumenteerd. Zo bleek uit een experiment met TikTok-testaccounts die 13-jarige gebruikers nabootsten, dat in één geval al binnen 2 minuten en 38 seconden een video over zelfdoding werd aanbevolen, nadat onderzoekers belangstelling hadden getoond in content over lichaamsbeeld en mentale gezondheid.[33] Een gelijkaardig experiment bracht een onderzoeker binnen drie uur van motiverende video's

31 Crone, E. A., & Konijn, E. A. (2018). Media use and brain development during adolescence. *Nature Communications, 9*, 588.

32 Boniel-Nissim, M., et al. (2024). *A focus on adolescent social media use and gaming in Europe, central Asia and Canada: Health Behaviour in School-aged Children international report from the 2021/2022 survey* (Vol. 6). WHO Regional Office for Europe.

33 Center for Countering Digital Hate. (2022). *Deadly by design: TikTok pushes harmful content promoting eating disorders and self-harm into users' feeds*. Deze bevindingen zijn later bevestigd in: Amnesty International. (2025). *Dragged into the rabbit hole: New evidence of TikTok's risks to children's mental health*.

over zelfverbetering tot expliciet misogyne content en rechtsextremistische narratieven.[34] Het Institute for Strategic Dialogue (ISD) laat zien dat het TikTok-algoritme zulke extremistische content ook ongehinderd verspreidt: een account dat interesse in radicaalrechtse denkbeelden nabootst, kreeg binnen mum van tijd drie video's van expliciete nazipropaganda aanbevolen.[35] Extremistische bewegingen spelen ook bewust in op de werking van dit algoritme. Bijvoorbeeld aanhangers van ISIS en al-Qaida verpakken hun propaganda in aantrekkelijke memes en filmpjes die niet alleen de moderatie passeren maar ook makkelijker meeliften op wat al viraal is.[36]

Criminele toeleidingspaden? Onderzoek naar criminele toeleidingspaden op sociale media en specifiek TikTok is schaarser. De eerder aangehaalde studie voor Politie & Wetenschap liet zien dat bijna één op de vijf jongeren tussen de 16 en 27 jaar op sociale media weleens een oproep heeft gezien waarin personen werden gezocht voor het uitvoeren van drugshandel of geweld, 6 procent zegt daarvoor actief benaderd te zijn.[37] Dit betekent niet dat elke jongere die zulke content tegenkomt er ook op ingaat. Traditionele factoren zoals leefmilieu, sociale omgeving en netwerk blijven een rol spelen in de vatbaarheid voor crimineel gedrag. Sociale media lijken hierin een duale rol te vervullen: enerzijds versterken ze identiteitsvorming en normalisering van een criminele levensstijl, anderzijds brengen ze vraag en aanbod sneller en over een groter geografisch bereik bij elkaar.

3.2. Blootstelling aan criminele content op TikTok

Om het proces van identiteitsvorming en normalisering van criminaliteit op TikTok in beeld te brengen, zijn twee verkennende experimenten uitgevoerd. Voor het eerste experiment is gebruik gemaakt van een nieuw en daarmee 'schoon' TikTok-account. Voor specifiek dit account zijn de eerste duizend aanbevolen video's gewogen op mogelijk inhoudelijke criminele content. Elke video is vervolgens gerangschikt op basis van onderstaande niveaus, oplopend van neutrale content tot het bevatten van expliciete criminaliteit of criminele diensten. Daarnaast werd geregistreerd of video's gebruikers doorverwezen naar andere socialemediaplatformen zoals Snapchat of Telegram. Deze doorverwijzingen komen in het volgende hoofdstuk apart aan bod.

Het tweede verkennende experiment volgde dezelfde escalatieladder, maar vertrok vanuit een ander uitgangspunt. In plaats van een volledig vers account werd hier gewerkt met vijf accounts waarbij gestart werd met een initiële, niet-criminele zoekterm, zoals "geld". Waar het eerste experiment inzicht gaf in hoe snel een account zonder enige initiële sturing 'vervuild' raakt met criminele of criminaliteit normaliserende content, wilde het tweede verkennende experiment bekijken of het aangeven van een neutrale zoekterm er ook voor zorgt dat er sneller ondeugdelijke content aangeboden wordt.

---

34 Dhoest, A. (2025). From manosphere to mainstream: Representations of masculinity on TikTok. *International Journal of Communication, 19*, 2201–2220.

35 Doctor, N., Fiennes, G., & O'Connor, C. (2024). *NazTok: An organized neo-Nazi TikTok network is getting millions of views*. Institute for Strategic Dialogue.

36 Karo, G., Divon, T., & Hallinan, B. (2026). The TikTok caliphate: How jihadist supporters exploit algorithmic recommendations and evade content moderation. *Social Media + Society, 12*(1).

37 Bergers, J., Van Deuren, S., Roks, R., Habets, S., Leukfeldt, E. R., & Eichelsheim, V. I. (2026). *De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit* (Politiekunde 133). Politie en Wetenschap, p. 48.

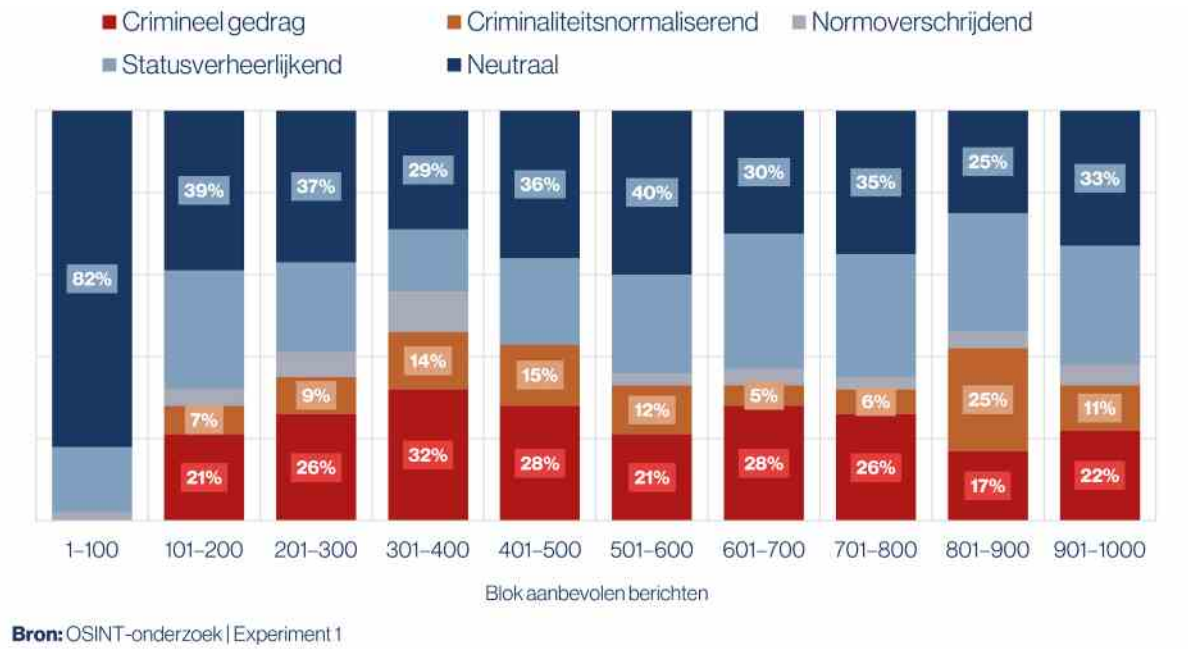
Tabel 1. Escalatieladder criminele content

Niveau	Beschrijving
0 – Neutraal	Geen normoverschrijdende of criminele elementen.
1 – Statusverheerlijkend	Aanprijzing van levensstijl waarin snel geld, gangstergedrag, enz. centraal staan.
2 – Normoverschrijdend	Aanmoediging tot het breken van regels of illegale activiteiten.
3 – Criminaliteitsnormaliserend	Verleidend tot concreet crimineel of gewelddadig gedrag.
4 – Crimineel gedrag	Expliciet getoonde criminele en/of illegale handelingen, methoden of diensten

Criminele content verschijnt na de eerste 100 posts. Onderstaande figuur laat zien dat de nieuwe account al zeer snel (na 102 posts) terechtkwam in content met concrete criminele handelingen en diensten. Waar in de eerste 100 posts nog 82 procent van de aanbevolen video's neutraal zijn, is dit in het volgende blok van 100 post slechts 39 procent. Waar lifestyle- en statusgerichte content direct al aan de orde is, volgen na de eerste 100 video's de eerste concrete video's met expliciete criminaliteit of diensten (21 procent). Het percentage video's in de feed met daarin normalisering en expliciete criminaliteit stijgt op naar 46 procent, waarna dit stabiel blijft hangen rond een derde van de aanbevolen video's.

Figuur 2. Escalatie criminele content op *For You* pagina TikTok

Percentage video's per niveau.



Bron: OSINT-onderzoek | Experiment 1

Van identiteit naar criminaliteit. De escalatie van criminele content in de feed van ons test-account doet in een aantal opzichten denken aan de geleidelijke weg waarlangs jongeren offline betrokken raken bij criminaliteit. Die betrokkenheid begint zelden met een strafbaar feit. Jongeren met specifieke risicofactoren zijn gevoelig voor een geromantiseerd beeld van een criminele levensstijl waarin status, geld en macht centraal staan. In een directe omgeving en

sociaal netwerk waarin criminaliteit een zichtbare route is naar die levensstijl, raakt criminaliteit genormaliseerd. Vaak volgt pas na deze normalisering de eerste criminele klusjes en handelingen.[38] Hoewel onderstaande route is gebaseerd op de resultaten van één testaccount, geeft het een indruk van hoe een vergelijkbare ontwikkeling zich online in 132 posts kan voltrekken:

- ***Post 6 – Statusverheerlijkend:*** Het algoritme probeert in de eerste posts duidelijk te begrijpen wat de interesses van de gebruiker zijn: aanbevelingen lopen uiteen van eten en *popculture* tot video's met een anti-institutioneel of rechtsextremistisch karakter. Al na 6 video's passeert de eerste post die inspeelt op het gevoel buiten de reguliere samenleving en haar normen te staan. Daarna volgen meer video's waarin makers benadrukken enkel op zichzelf te kunnen vertrouwen en niet te zijn zoals "de rest". Tegelijkertijd verschijnen er video's waarin wordt gepronkt met nepgeld, horloges, auto's en andere materiële zaken. In *edits* worden krachtige en weerbare figuren zoals boksers bewonderd. Het algoritme speelt in op het gevoel "er niet bij te horen", en zet daar een geïdealiseerde identiteit tegenover die draait om status, (financiële) onafhankelijkheid en macht.
- ***Post 59 – Normoverschrijdend:*** Onafhankelijkheid en status vallen in de feed al snel samen met een afkeer van heersende maatschappelijke normen en autoriteit. Na 59 posts verschijnen de eerste video's waarin de politie belachelijk wordt gemaakt, bijvoorbeeld met beelden van aanhoudingen of brutaal gedrag richting de politie. Andere posts zetten tegenover het contact met de politie de ongestoorde voortzetting van een vrije en luxe levensstijl. De onderliggende boodschap is dat het gezag er voor hen niet toe doet.[39] Status en macht blijken daarmee ook buiten de geldende normen bereikbaar.
- ***Post 102 – Criminaliteitsnormaliserend:*** Normvervaging slaat al snel om in het verheerlijken en daarmee normaliseren van daadwerkelijke criminaliteit. In de feed komen video's naar voren die beruchte criminelen zoals Ridouan Taghi en Bolle Jos in een positief licht zetten. Daarnaast komen er beelden voorbij van overvallen, brandstichting, bedreigingen en inbraak. Deze handelingen worden bewonderd en omschreven met verheerlijkende termen zoals "strijders" of "soldaten". In deze fase gaat het nog om bewondering voor deze criminele activiteiten, niet om werving of instructies. Een aparte categorie omvat content rondom het gevangenisleven. Hierin komt bijvoorbeeld de smokkel van verboden spullen de gevangenis in naar voren, of wordt het leven in de gevangenis afgeschilderd als comfortabel. Het algoritme biedt zo een wereldbeeld aan waarin misdaad status oplevert en gevangenschap eerder bij die levensstijl hoort dan dat het afschrikt.
- ***Post 132 – Crimineel gedrag:*** Na slechts 132 aanbevolen TikToks toont de feed video's waarin criminele hulpmiddelen worden verkocht, instructies voor criminele handelingen worden gegeven en verboden middelen worden aangeboden. Het gaat daarbij om hulpmiddelen zoals inbraakwerktuig, signaalblokkers, objecten met verborgen bergruimtes, aangepaste drones, tabletteermachines en 3D-geprinte pistoolonderdelen. Ook worden instructies gegeven voor bijvoorbeeld het produceren van drugs, het openbreken van sloten en het maken van wapens uit reguliere gebruiksvoorwerpen. Daarnaast werd er geadverteerd voor de verkoop van drugs en voor "signal sweep" diensten die auto's of woningen controleren op verborgen GPS-trackers of afluisterapparatuur. Op dit niveau reikt het algoritme naast een identiteit en een alternatief normenkader ook de middelen, kennis en contacten aan om die criminele wereld daadwerkelijk in te stappen.

Op de volgende bladzijde is de opbouw in blootstelling aan criminele content op TikTok voorzien van enkele illustraties uit het OSINT-onderzoek.

---

38 Adjiembaks, S. D., Boer, A. H., & Oude Lansink, M. J. (2022). *(On)zichtbare beelden van jonge aanwas in de drugscriminaliteit: Een meta-analyse van tien deelonderzoeken in de regio Midden-Nederland*. RIEC Midden-Nederland & ESSA Research.

39 Door deze antiautoritaire houding komen in de feed ook anti-institutionele en enkele complotnarratieven naar voren.

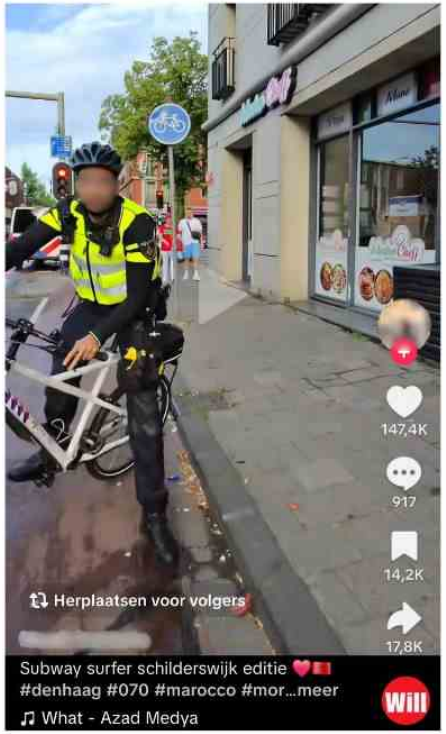
Blootstelling aan criminele content op TikTok

Escalatiepad met een nieuw TikTok-account



Post 6

Statusverheerlijkend
Video's spelen in op het gevoel er niet bij te horen. Ze bieden een geïdealiseerde identiteit gebaseerd op status, onafhankelijkheid en macht.



Post 59

Normoverschrijdend
Gezag en autoriteit worden afgewezen als hindernis voor een onafhankelijke en luxe levenstijl.



Post 102

Criminaliteitsnormaliserend
Criminelen en criminele daden worden verheerlijkt. Misdaad levert status op, gevangenschap schrikt niet af.



Post 132

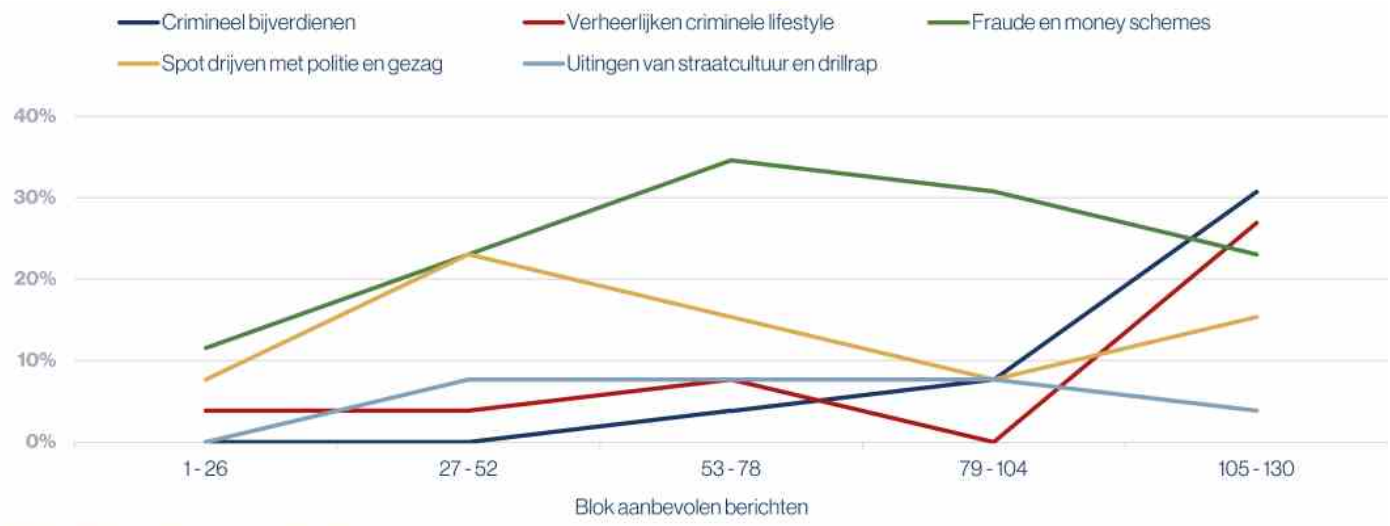
Crimineel gedrag
De feed biedt concrete middelen, kennis en diensten om zelf in de criminaliteit te stappen of deze af te nemen.

Bron: OSINT-onderzoek | Experiment 1

Aard en zwaarte van criminele content is afhankelijk van gebruikersinteresse. Het tweede experiment simuleerde vijf gebruikers met specifieke niet-criminele interesses maar met zoektermen die wel hinten aan de vijf contenttypen besproken in hoofdstuk 2.[40] Ook hier is zichtbaar hoe interactie snel leidt tot aanbevelingen van criminele content. Bij vier van de vijf profielen liep het aandeel criminele content in de feed op tot ten minste 10 procent aan het einde van het experiment, bij de thema's bijverdienen en ondernemerschap piekte dit percentage gedurende het experiment boven de 30 procent. Enkel binnen het thema straatcultuur bleef het percentage criminele content in de feed stabiel rond de 8 procent.

Figuur 3. Escalatie criminele content naar gebruikersinteresse

Percentage posts dat criminaliteitsnormaliserend is of crimineel gedrag toont.



Bron: OSINT-onderzoek | Experiment 2

Het korte experiment laat zien dat de initiële gebruikersinteresse in belangrijke mate de aard en zwaarte van de aanbevolen criminele content bepaalt. Een gebruiker geïnteresseerd in financiën en ondernemerschap escaleerde het snelst naar crimineel gedrag in de vorm van 'hustle-guru's', nepproducten en cryptoscams.[41] Een gebruiker die zoekt naar manieren om wat geld bij te verdienen, kreeg in de eerste 52 posts juist geen enkele criminele aanbeveling, maar kreeg daarna al snel video's te zien met handel in nepgeld en illegale vapes, en andere verdienmodellen die overlappen met die van ondernemerschap.[42]

Wie neutraal zoekt naar video's over politie en vervolgens de feed ververst stuit snel op gezagsondermijnende content. Expliciet crimineel gedrag verschijnt dan juist minder duidelijk op de feed. Opvallend is ten slotte het item 'straat', verwijzend naar straatcultuur.[43] Hoewel straatcultuur, en in het verlengde daarvan drillrap, regelmatig in verband worden gebracht met geweld en criminaliteit, bleef de feed van dit profiel het verst verwijderd van crimineel gedrag in de feed. Muziekvideo's over het leven op straat verwijzen wel naar geweld of criminaliteit,

40 Deze interesse is gesimuleerd door met een nieuw account eerst te zoeken op een bepaalde zoekterm die verband houdt met het interessegebied.

41 Gesimuleerd met de zoekterm "geld".

42 Gesimuleerd met de zoekterm "verdienen".

43 Gesimuleerd met de zoekterm "straat".

maar tonen dit niet expliciet. De relatie tussen straatcultuur en criminele content is daarmee minder eenduidig dan wellicht wordt aangenomen. Dit past tevens bij de dubbele rol van creatieve uitingen op sociale media: ze kunnen crimineel gedrag normaliseren, maar ook een uitlaatklep bieden die kwetsbare jongeren juist van dat pad afhoudt.

De routes waarmee gebruikers terecht komen in een crimineel contentmilieu zijn dus divers. Gezien de werking van het algoritme is dat weinig verrassend, maar het betekent wel dat online interventies zich slecht lenen voor één standaardaanpak. Wie op één herkenbare route inzet, mist gebruikers die via andere interesses in criminele content terechtkomen.

3.3. **Contentmoderatie op TikTok**

Dat criminele content zo makkelijk in de feed belandt, roept de vraag op hoe TikTok hier zelf mee omgaat. Het platform verbiedt in zijn Community Guidelines onder meer het verheerlijken van geweld, het promoten van misdaad, het delen van instructies voor misdrijven en de handel in drugs, wapens, nepgeld en andere verboden goederen.[44] Handel is daarbij ruim gedefinieerd en omvat ook het doorverwijzen naar andere platformen.

Volgens TikTok worden overtredingen grotendeels automatisch opgespoord. In het tweede kwartaal van 2026 verwijderde het platform wereldwijd ruim 188 miljoen video's, ongeveer 0,5 procent van alle uploads. Ruim 99 procent daarvan zou zijn verwijderd voordat een gebruiker er melding van maakte.[45] Die cijfers zeggen echter niets over de content die de automatische detectie passeert. Daarvoor is het platform afhankelijk van meldingen van gebruikers. Om te toetsen hoe dat vangnet werkt, is een derde verkennend experiment uitgevoerd. Honderd posts die naar ons oordeel de Community Guidelines schenden en normaliserende dan wel expliciete criminaliteit vertonen, zijn via de meldfunctie van de app gerapporteerd.[46] Vervolgens is bijgehouden hoe TikTok de meldingen afhandelde.

Vier op de vijf gemelde posts blijven ongemoeid. Van de honderd gemelde posts beoordeelde TikTok dat er bij 81 geen sprake was van een schending van de community guidelines. Die posts bleven ongewijzigd online en konden in de For You-feed blijven verschijnen. Bij 11 posts verwijderde TikTok de content. Bij 7 posts werd de verspreiding beperkt: de video bleef staan, maar werd niet langer aanbevolen in de For You-feed. Eén post werd tussentijds door de maker zelf verwijderd. Bij minder dan een vijfde van de meldingen volgde dus enige maatregel.

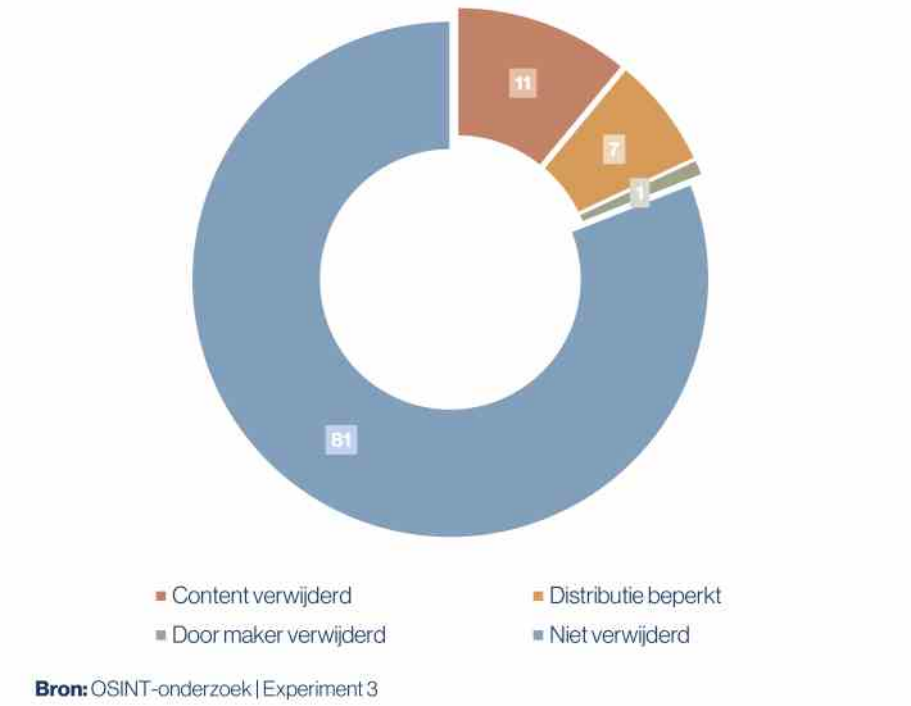
---

44 TikTok. (2026a). *Community guidelines* (versie van 25 augustus 2026, van kracht sinds 24 september 2026). Relevant zijn met name de secties 'Violent and Criminal Behavior', 'Violent and Hateful Organizations and Individuals', 'Regulated Goods and Services', 'Frauds and Scams' en 'Enforcement'.

45 TikTok. (2026c). *Community guidelines enforcement report: April–June 2026*. TikTok Transparency Center.

46 De posts zijn gemeld via de standaard meldfunctie in de app, afhankelijk van de content bijvoorbeeld onder "geweld, misbruik en criminele uitbuiting", "namaakproducten verkopen", "gereguleerde goederen en activiteiten" of "fraude en oplichting". De uitkomst per melding is vastgesteld op basis van de terugkoppeling die TikTok aan de melder geeft. Deze terugkoppeling kwam soms na enkele minuten, maar meestal binnen twee tot drie dagen.

Figuur 4. Verwijderde posts met criminele content na rapportage



Bron: OSINT-onderzoek | Experiment 3

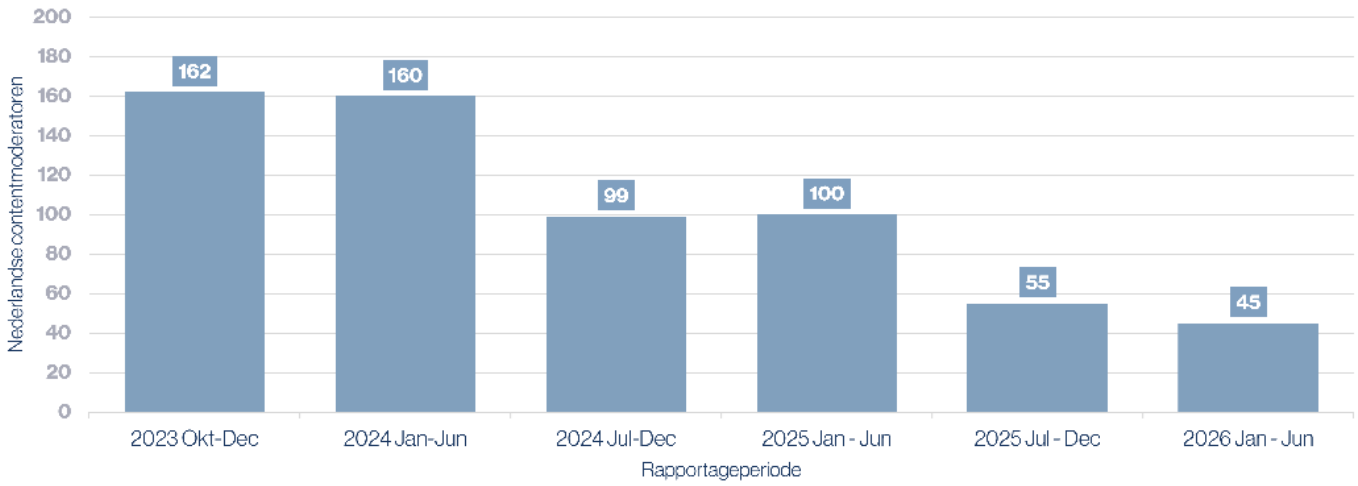
Wat zeggen de richtlijnen? Dat TikTok 81 meldingen afwees, betekent niet dat deze posts binnen de regels vallen. Volgens de Community Guidelines schenden elk van de honderd posts direct, dan wel met hun meer impliciete boodschap, ten minste één verbodsbepaling. Het gaat in beginsel niet om onduidelijke twijfelgevallen maar om video's die nadrukkelijk geweld of crimineel gedrag verheerlijken, die verboden goederen aanbieden of naar een verkoopkanaal verwijzen, of die instructies geven voor illegale handelingen. De richtlijnen kennen wel uitzonderingen. Documentaire en educatieve content over geweld en criminaliteit is toegestaan, net als fictie, kunst en kritiek op crimineel gedrag. Ook vechtsport of geweld waarvan duidelijk is dat het niet echt is, valt niet onder het verbod. Nieuwsfragmenten zijn toegestaan omdat ze vastleggen wat er is gebeurd.

Die uitzonderingen hangen echter af van het doel van de post, niet van het beeldmateriaal als zodanig. Een deel van de gemelde posts gebruikt bijvoorbeeld een nieuwsfragment over een overval als meme, met een tekst in de trant van 'zodra je gaat trouwen en geld nodig hebt'. Het beeldmateriaal is journalistiek van herkomst, maar wordt in de post voor iets anders ingezet. Wanneer de begeleidende tekst de daders bewondert, criminaliteit aantrekkelijk voorstelt, anderen aanspoort hetzelfde te doen, uitlegt hoe het werkt of verwijst naar waar middelen te krijgen zijn, valt de post alsnog onder het verbod op het promoten van criminaliteit. Op dezelfde manier blijft een video waarin inbraakgereedschap wordt aangeboden voor wie 'zijn sleutels kwijt is' een aanbod van inbraakgereedschap.

Hoe valt het verschil te verklaren? Er is ruimte voor interpretatie, en bij een deel van de posts kan TikTok redelijkerwijs tot een andere afweging komen dan wij. Een verschil van deze omvang laat zich daarmee echter niet verklaren. Aannemelijker is dat bij de beoordeling de context ontbreekt die de betekenis van een post bepaalt: het bijschrift, de muziek, de emoji, de verwijzing in de bio of de gecodeerde termen die makers bewust kiezen om moderatie te omzeilen. Die context is bovendien vaak Nederlandstalig en doorspekt met straattaal, terwijl TikTok sinds 2023 het aantal Nederlandstalige moderatoren heeft gereduceerd van 162 naar

45 in 2026. Of meldingen door mensen of door systemen worden beoordeeld, maakt TikTok niet inzichtelijk. Opvallend is ook dat de lichtere maatregel, het uitsluiten van de For You-feed, nauwelijks werd ingezet. Die maatregel is juist bedoeld voor content die niet verboden is, maar waarvan het ook niet wenselijk wordt geacht deze aan een breed publiek te tonen. Voor veel van de borderline content uit hoofdstuk 2 had dat een voor de hand liggende tussenweg kunnen zijn.

Figuur 5. Nederlandse contentmoderatoren TikTok



Bron: TikTok Digital Services Act Reporting

Melden van content als primair vangnet. Voor beleid is deze uitkomst relevant, omdat melden bij het platform zelf het belangrijkste vangnet is voor content die de automatische detectie passeert. Het experiment suggereert dat dit vangnet in het geval van TikTok dus grote gaten heeft. Wat aan de voorkant niet wordt herkend, blijft na een melding vaak alsnog staan, ondanks dat de Digital Services Act platformen al verplicht meldingen serieus te behandelen. Zo kunnen gebruikers content niet alleen melden als overtreding van de huisregels van het platform, maar ook als illegale inhoud, die het platform dan aan het nationale recht moet toetsen. Daarnaast kunnen erkende organisaties de status van betrouwbare 'flagger' krijgen, waardoor platformen hun meldingen met voorrang moeten behandelen.[47] In Nederland wees de ACM in juli 2025 de eerste betrouwbare flagger aan: Stichting Offlimits, die zich richt op online seksueel grensoverschrijdend gedrag.[48] Later dat jaar volgden Brein, Meld Online Discriminatie en React.[49] Een vergelijkbare rol voor organisaties met expertise op het gebied van criminele content en online werving ligt voor de hand (zie paragraaf 5.1). Beide regels dwingen echter tot een beoordeling, nog niet per definitie tot verwijdering: het platform blijft de afwegingen baseren op de eigen richtlijnen.

Kanttekening. Het uitgevoerde experiment is nadrukkelijk verkennend. Het gaat om honderd posts die door de onderzoekers zelf zijn geselecteerd en beoordeeld, en de uitkomst is niet zonder meer te generaliseren naar alle meldingen op TikTok. Ook is niet bekend hoe TikTok de meldingen precies heeft beoordeeld.

47 Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten (digitaledienstenverordening), *PbEU* 2022, L 277, art. 16 en 22.

48 Autoriteit Consument & Markt. (2025, 22 juli). *Aanwijzingsbesluit status betrouwbare flagger voor Stichting Offlimits*. ACM.

49 Autoriteit Consument & Markt. (2025, 1 oktober). *Aanwijzingsbesluit status betrouwbare flagger voor Brein, Meld Online Discriminatie en React*.

4. Snelweg naar crimineel *handelen*?

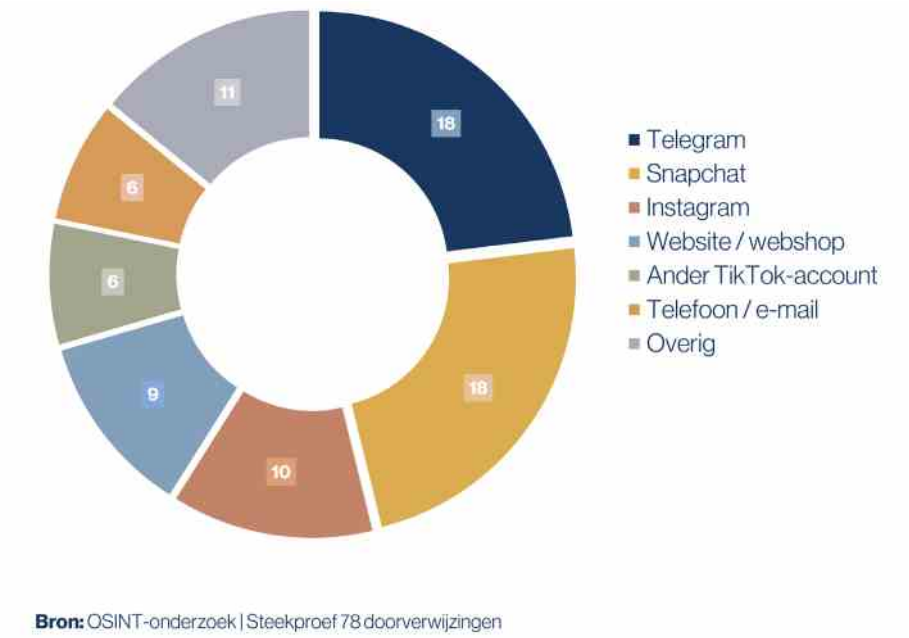
Het vorige hoofdstuk toonde hoe jongeren met verschillende achtergronden en interesses via algoritmische aanbevelingen in aanraking kunnen komen met content die criminaliteit expliciet toont. Dit hoofdstuk richt zich op de vraag in hoeverre aangetroffen content doorverwijzingen aanbiedt richting andere netwerken en besloten groepen, met het idee dat daar concretere criminele werving kan plaatsvinden of illegale aanbiedingen kunnen worden gedaan.

4.1. Van open platform naar afgeschermd kanaal

In het online criminele ecosysteem vervullen platformen verschillende functies. Open platformen zoals TikTok leveren bereik op en dragen bij aan normalisering. Een deel van de accounts die deze criminele content verspreiden, wijzen geïnteresseerde gebruikers door naar privéchats of andere kanalen op bijvoorbeeld Snapchat, Instagram of Telegram. In deze afgeschermde omgevingen kan blootstelling langs twee routes omslaan in betrokkenheid. Aan de ene kant posten ronselaars hier vaag omschreven oproepen voor het uitvoeren van een klus, met de uitnodiging om bij interesse privé te reageren. Maar jongeren worden ook actief benaderd door onbekenden. Het eerder aangehaalde onderzoek onder Nederlandse jongeren identificeert hoofdzakelijk Snapchat, TikTok, Whatsapp en Instagram als kanalen waarop jongeren direct zijn benaderd voor het uitvoeren van een drugs- of geweldsdelict.[50]

[50] Bergers, J., Van Deuren, S., Roks, R., Habets, S., Leukfeldt, E. R., & Eichelsheim, V. I. (2026). *De rol van social media in de betrokkenheid van jongeren bij zware en georganiseerde drugs- en geweldscriminaliteit* (Politiekunde 133). Politie en Wetenschap, p. 46.

Figuur 6. Doorverwijzingen op TikTok
Vanaf accounts met criminele content



Bron: OSINT-onderzoek | Steekproef 78 doorverwijzingen

Doorverwijzingen op TikTok. Het OSINT-onderzoek voor deze HCSS Focus beperkt zich tot de doorverwijzingen naar andere kanalen die zijn gevonden op TikTok. Op basis van een steekproef van 119 TikTok-accounts met criminaliteit verheerlijkende of expliciet criminele content is nader geanalyseerd of deze accounts gebruikers doorleiden naar andere kanalen, welke kanalen dit zijn en wat voor soort content daar is aangetroffen. Bij 53 van de geanalyseerde accounts zijn in totaal 78 platformvermeldingen aangetroffen. Het merendeel van deze doorverwijzingen staat in de biografie van het desbetreffende TikTok-account. Doorverwijzingen zijn ook gevonden in reacties, in beeld of gesproken tekst van de video, in onderschriften of via herkenbare gebruikersnamen.

Telegram en Snapchat ontvingen in deze steekproef elk bijna een kwart van de doorverwijzingen vanuit TikTok-accounts met criminele content. Hoewel de doorverwijzingen in kwantiteit gelijk zijn, verschilt de aard van deze doorverwijzingen. Snapchat werd meestal gebruikt voor direct persoonlijk contact, vanuit de zichtbare profielen ontstond geen uitgebreidere netwerkstructuur. Op Telegram kwamen daarentegen meerdere functies samen in dezelfde omgeving. Openbare kanalen verzamelen daar volgers, tonen aanbod van goederen en diensten, verwijzen gebruikers door naar andere accounts en kondigen nieuwe en back-up accounts aan. De gebruiker kwam daardoor niet bij één contactpersoon terecht, maar kreeg toegang tot een breder netwerk. Vanuit deze Telegramkanalen bestaan legio mogelijkheden voor een-op-een contact met specifieke gebruikers, wat buiten de scope van deze steekproef ligt.

Doorverwijzingen naar Instagram ondersteunden vooral de herkenbaarheid en identiteit van het desbetreffende TikTok-account. Het profiel fungeert als het ware als een extra portfolio en levert zo extra bereik op. Verwijzingen naar andere TikTok-accounts dienden als back-up, targeten een andere doelgroep of vervingen een al verwijderd account. Beide routes blijven binnen de publieke laag en houden de digitale identiteit van een account intact, ook wanneer een individueel account verdwijnt. In een klein deel van de gevallen verliep de doorverwijzing niet rechtstreeks, maar via diensten als Linktree, Hoo.be of Biosites. Deze diensten bundelen bestemmingen in een tussenstap zonder dat meteen zichtbaar is naar welk platform een verwijzing uiteindelijk leidt.

4.2. Strategische werving door criminele netwerken

Wat er gebeurt nadat een gebruiker één van de hierboven geïllustreerde routes neemt, blijft in deze verkenning in beginsel buiten beeld. Maar Europese en Nederlandse onderzoeken geven wel de nodige indrukken over hoe werving voor criminele klussen plaatsvindt en hoe vaak.

Europese data: minderjarigen actief in 70 procent van criminele markten. In november 2024 publiceerde Europol een inlichtingenbrief waarin het waarschuwde voor de rekrutering van jonge daders voor criminele netwerken.[51] Hierin schreef het agentschap dat minderjarigen inmiddels actief zijn in 70 procent van de criminele markten waaronder cybercrime en online fraude, drugscriminaliteit, mensensmokkel en inbraak. Het gebruik van deze jongeren is functioneel en strategisch. Zij hebben meestal geen kennis van het bredere criminele netwerk en lopen door het ontbreken van een strafblad minder snel in het oog van de autoriteiten. Online platformen spelen daarbij ook volgens Europol een belangrijke aandrijvende en faciliterende rol in de rekrutering, van drugsuithaal tot geweld-op-bestelling (Violence as a Service, of VaaS).[52] Tussen april 2025 en april 2026 arresteerde Europol in samenwerking met verschillende lidstaten 280 personen op verdenking van het ronselen van jongeren. Bijna tweederde daarvan wordt verdacht van rekrutering. Daarnaast heeft het nog zo'n 14.000 accounts in beeld die betrokken zijn bij deze netwerken.[53]

De trend van VaaS is het sterkst gedocumenteerd in Zweden. Onder 15 tot 20-jarigen steeg het aantal verdachten van moord, doodslag en zware mishandeling met een dodelijke afloop van 34 in 2014 naar 167 in 2023. Een stijging van bijna 400 procent, terwijl deze voor de groep boven de 21 beperkt bleef tot 37 procent. In 2024 zouden er volgens de Zweedse politie ongeveer 1700 minderjarigen actief betrokken zijn bij criminele netwerken, ongeveer 13 procent van alle deelnemers.[54] Naar aanleiding van de toename van gevallen waarin criminele netwerken minderjarigen via sociale media rekruteerden en inzetten voor geweldsdelicten wil de Zweedse regering de leeftijd waarop kinderen strafrechtelijk vervolgd kunnen worden, verlagen naar 14 jaar.[55]

Het Nederlandse beeld: jonge aanwas meest zichtbaar bij explosievenleggers. De online werving van Nederlandse jongeren voor de georganiseerde criminaliteit moet worden bezien tegen de achtergrond van een halvering van de jeugdcriminaliteit in de afgelopen twee decennia. In de Monitor Jeugdcriminaliteit (2000-2023) nuanceert het WODC de claim dat jongeren betrokken zijn bij steeds ernstigere of gewelddadigere criminaliteit; recente onderzoeken zien deze trend "maar beperkt en dan enkel op de korte termijn" terug.[56] Kijkend naar de ontwikkelingen sinds de coronaperiode is het wel opvallend dat de bredere afname in criminaliteit voor de meeste leeftijdsgroepen doorzet, maar voor minderjarigen vanaf 12 jaar stabiliseert dan wel omslaat. Dit is het sterkst waarneembaar bij het aantal geregistreerde verdachten van geweldsmisdrijven en in mindere mate bij (vuur)wapenmisdrijven. Bij drugsmisdrijven zet de afname in verdachten ook onder minderjarigen door.[57]

---

51 Europol. (2024). *The recruitment of young perpetrators for criminal networks* (intelligence notification). Europol.

52 Luyten, K., & Baltikauskaite, G. (2025). *Recruitment of minors into organised crime*. European Parliamentary Research Service.

53 Schrader, M., & Linssen, F. (2026, 28 april). Europol: 280 verdachten opgepakt voor ronselen jongeren voor 'geweld op bestelling'. *NOS*.

54 Ekman, T. (2025). *Alarming rise in youth crime in Sweden: Young people increasingly involved in criminal networks*. IJAB – International Youth Service of the Federal Republic of Germany.

55 NOS. (2026, 11 juni). *Zweedse regering buigt: cel voor 13-jarigen gaat niet door, mikt nu op 14-jarigen*.

56 Van der Laan, A. M., Tollenaar, N., Beijers, J., & Kessels, R. (2024). *Ontwikkelingen in de jeugdcriminaliteit* (Cahier 2024-15). WODC, p. 40.

57 Centraal Bureau voor de Statistiek (CBS). (2026b). *Verdachten; delict, leeftijd, geslacht en woongemeente* (dataset). CBS StatLine.

Figuur 7. Verdachten van geweld per leeftijdscategorie
Procentuele verandering 2020-2025



Bron: CBS

Op de korte termijn is er onder minderjarigen dus een stabilisatie dan wel groei in de betrokkenheid bij specifieke criminele delicten te zien. Dit roept de vraag op of deze stabilisatie verband houdt met de verspreiding van criminele content op sociale media zoals TikTok en de betrokkenheid van jongeren bij de georganiseerde misdaad. Huidige cijfers geven hier geen antwoord op. Wel is dit patroon duidelijk waarneembaar in de groei van aanslagen met explosieven, van 212 in 2021 naar 1525 in 2025.[58] In de eerste helft van 2026 was 45 procent van de aangehouden verdachten voor dit feit minderjarig.[59] Een zaak in Alkmaar illustreert hoe tieners via onder andere Snapchat werden benaderd en aangestuurd voor het plegen van zulke aanslagen.[60] Ook voor de aanslag in Overasselt in september 2026 werden op Snapchat extra deelnemers geworven met het bericht "Yo soldaat, ik heb boys nodig. 10K per man." De instructies volgden via Snapchat en Signal, waarbij de opdracht in de loop van de chats verschoof van iemand in elkaar slaan naar dodelijk geweld.[61]

DZ Mafia: grensoverschrijdende werving. In het OSINT-onderzoek werd ook Franstalige content aangetroffen, deels herleidbaar tot Marseille. In die stad heeft zich de zogenaamde DZ Mafia (Dyazir) ontwikkeld, een inmiddels Europabreed verspreid crimineel netwerk dat sociale media uiterst tactisch inzet voor ronseling, communicatie en netwerkmanagement. Snapchat en TikTok zijn voor DZ ideale platformen om minderjarigen te bereiken. Minderjarigen zijn ideaal om te werven omdat ze vanwege het jeugdstrafrecht in Europese landen vaak snel weer op vrije voeten staan. Ze werken voor kleine bedragen en zijn flexibel inzetbaar. Soms wordt ook wel gesproken over überisering van georganiseerde misdaad vanwege het decentrale sturingsmodel. DZ breidt zijn activiteiten momenteel uit naar meer noordelijke delen van Europa. Belgische autoriteiten hebben gewaarschuwd voor activiteit in Brussel en Antwerpen. Het succes van DZ onderschrijft mogelijk dat de wervings- en selectietactieken effectief zijn en wellicht meer navolging zullen vinden in andere criminele samenwerkingsverbanden. Het lijkt er in ieder geval op dat deze verbanden niet blind zijn voor de 'tooling' van socialemedia-infrastructuur voor hun belangen.[62]

58 Politie. (2026). *Lichte daling aantal aanslagen met explosieven in 2025*.

59 Offensief tegen Explosies. (2026). *Factsheet januari tot en met juni 2026*.

60 Openbaar Ministerie. (2026). *Tot tien jaar gevangenisstraf geëist tegen drie verdachten van opdracht geven tot explosies in Alkmaar*.

61 Oogjes, M. (2026, 2 oktober). *'10K per man': zo werd groep gevormd voor schietpartij Overasselt*. Omroep Gelderland.

62 Leestmans, D. (2025, 8 maart). 'The French connection' in Brussel: Welke links zijn er met Marseille en hoe pakken ordediensten er drugsgeweld aan? *VRT NWS*; Carlier, M. (2025, 1 december). «La DZ mafia s'implante»: À Bruxelles, l'inquiétude grandissante des riverains et des autorités face à l'arrivée des narcotrafiquants marseillais. *Europe 1*.

5. Op zoek naar een antwoord

De uitkomsten van deze verkenning – ook al gaat het om een momentopname – illustreren dat een willekeurige, ongeprofileerde gebruiker binnen korte tijd in aanraking kan komen met criminele content op TikTok. Bovendien blijkt dat verwijderverzoeken op basis van onze geselecteerde content maar nauwelijks worden opgevolgd. We willen ons tot slot richten op de vragen waarom de aanpak soms wordt gehinderd en waar we op dit moment op in zouden kunnen zetten als we op een realistische manier meer regie zouden willen krijgen over het criminele contentaanbod. Het gaat om een indicatieve strategische richting. We pretenderen niet dat met deze ideeën een sluitende oplossing in het vooruitzicht ligt.

5.1. Vijf V's van de aanpak van digitale criminele content

Socialemediaproblematiek aanpakken vergt altijd meersporenbeleid. De hier door ons voorgestelde ordening van sporen waarover die aanpak kan verlopen is grosso modo geïnspireerd op de Nationale Contraterrorisme Strategie 2022–2026, mede omdat de online dimensie daarin ook een belangrijk onderdeel van de problematiek vormt. Deze contraterrorismestrategie onderscheidde eerder al qua aanpak vier V's, namelijk: Verwerven, Voorkomen, Voorbereiden en Vervolgen.[63] Die systematiek biedt een bruikbaar uitgangspunt vanwege het integrale perspectief en de ketenaanpak die het voorstelt. Juist op het vlak van digitale interventies zijn deze benaderingen logisch omdat de oorzakelijke factoren verspreid liggen over zowel de plaats als de tijd.

Ook de Versterkte Aanpak Online van de NCTV biedt aanknopingspunten. Die aanpak combineert onder andere samenwerking mét, en verantwoordelijkheid ván platformen. Daarbij wordt onder meer ingezet op betere contentmoderatie en het tegengaan van platformmigratie.[64] Hoewel die aanpak ook hier is gericht op extremistische content, zijn de onderliggende vraagstukken vaak vergelijkbaar als het gaat om het aanbod en de moderatie.

Een verdere onderbouwing bieden eerdere HCSS-onderzoeken "Het Com-netwerk" en "Van meme tot moord". Die studies lieten reeds zien hoe digitale subculturen, criminele netwerken en rekruteringsprocessen met elkaar verweven raken, waarbij bovendien de grenzen tussen online en offline handelingen dan wel criminaliteit, en tussen daderschap en slachtofferschap vervagen. De aanbevelingen benadrukten reeds het belang van structurele monitoring en inzet op OSINT-capaciteit, grotere platformverantwoordelijkheid, meer inzet op preventie en jeugdbescherming, en versterking van juridische en operationele interventiemogelijkheden.[65]

---

63 Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). (2022). *Nationale contraterrorisme strategie 2022–2026*. NCTV.

64 Kamerstukken II 2025/26, 29 754, nr. 774 (Voortgangsbrief Versterkte Aanpak Online inzake extremistische en terroristische content, 17 december 2025).

65 The Hague Centre for Strategic Studies (HCSS). (2026). *Het Com-netwerk* (HCSS Focus). HCSS.

Staand beleid. In Nederland lopen uiteraard al verschillende initiatieven. Vanuit het programma Preventie met Gezag lopen er in verscheidene gemeenten extra inspanningen op het voorkomen van (digitale) opname van jongeren in de georganiseerde criminaliteit. Ook lopen er andere en meer fundamentele onderzoeken zoals het programma "Online ronselen voor criminaliteit", onder de hoede van het Centrum tegen Kinderhandel en Mensenhandel. Het Centrum voor Criminaliteitspreventie en Veiligheid biedt gemeenten een routekaart voor samenwerking bij online jeugdcriminaliteit.[66] Deze initiatieven richten zich vooral op preventie, hulpverlening en lokale samenwerking. De platformverantwoordelijkheid krijgt verhoudingsgewijs minder aandacht. Vandaar dat we dit aspect explicieter hebben willen meenemen.

Voortbouwend op deze beleidsmatige en empirische inzichten stellen we vijf complementaire interventiegebieden voor.

Vijf strategische interventiegebieden, "vijf V's".

- *Verkennen: signaleren, monitoren en duiden.* Het vroegtijdig identificeren en doorlopend analyseren van criminele content, digitale ecosystemen, opkomende fenomenen en toeleidingspaden. Doel is inzicht te verkrijgen in criminele modus operandi, rekruteringsmechanismen en onderliggende digitale dynamieken.
- *Verantwoordelijk stellen: platformen aanspreken op hun rol*. Het stimuleren en waar nodig afdwingen van platformverantwoordelijkheid, onder meer via toezicht, samenwerking, contentmoderatie en het aanpakken van faciliterende algoritmische mechanismen. De Digital Services Act biedt hiervoor een belangrijk juridisch kader.
- *Voorkomen: criminele aanwas en slachtofferschap tegengaan.* Het tegengaan van online rekrutering, criminele socialisatie en normalisering van criminaliteit. Dit omvat digitale weerbaarheid, preventieve interventies en het beschermen van kwetsbare groepen, in het bijzonder jongeren.
- *Verstoren: criminele digitale processen doorbreken.* Het gericht aanpakken van criminele content, accounts, netwerken en infrastructuren. De inzet richt zich niet alleen op afzonderlijke uitingen, maar ook op achterliggende rekruteringsprocessen, verdienmodellen en criminele samenwerkingsverbanden.
- *Vervolgen: strafrechtelijke handhaving.* Het opsporen en vervolgen van personen en organisaties die via digitale platformen strafbare feiten plegen, voorbereiden of faciliteren, waaronder fraude, bedreiging, criminele uitbuiting en terroristische misdrijven.

Cyclisch proces. De vijf interventiegebieden versterken elkaar. Doorlopende signalering en duiding voeden platformgerichte, preventieve en repressieve interventies. Omgekeerd leveren deze interventies nieuwe inzichten op. Zo richt de aanpak zich zowel op de uitingen zelf als op de mechanismen die ze mogelijk maken.

66 Rijksoverheid. *Preventie met Gezag*; Centrum tegen Kinderhandel en Mensenhandel (CKM). (2026). *Online ronselen voor criminaliteit*; NHVeilig, Partner in Crime & CCV (2026), *Routekaart 2.0 Samenwerken bij online jeugdcriminaliteit.*

5.2. Knelpunten en strategische richtpunten

De vijf V's bieden een samenhangend handelingsperspectief, maar elk interventiegebied kent op dit moment belangrijke beperkingen. Hieronder bespreken we enkele kort per interventiegebied, telkens gevolgd door concrete stappen om deze beperkingen te verkleinen.

Aan beleidskaders ontbreekt het niet; de zwakke plek zit vooral in het soms beperkte vermogen om ze effectief door te zetten. Twee overkoepelende knelpunten zijn van terugkerende aard: een ontoereikende informatiepositie ten aanzien van snel veranderende digitale ecosystemen, en een asymmetrische machtsverhouding tussen overheden en internationale platformbedrijven. Vooral dat laatste is een structurele belemmering, zeker als het gaat om borderline content. Platformen ontsluiten criminele content en bepalen via hun ontwerp, aanbevelingssystemen en moderatiebeleid mede hoe criminele toeleidingspaden en normaliserende contentmilieus ontstaan en voortbestaan.

Verkennen: signaleren, monitoren en duiden van criminele content en toeleidingspaden. Een effectieve aanpak vraagt om diepgaande kennis van digitale subculturen, codetaal en veranderende criminele werkwijzen. Zoals ook al in de HCSS-studie Het Com-netwerk wordt vastgesteld in relatie tot online extremisme, ontbreekt die specialistische expertise nog geregeld of is ze afhankelijk van civiele OSINT-onderzoekers.[67] Daarnaast beperken afgeschermde chatgroepen, platformmigratie en juridische onzekerheid over stelselmatige monitoring de informatiepositie. Vooral vroegtijdig meekijken zonder concrete verdenking is ingewikkeld. Het gaat daarbij niet alleen om bevoegdheden, maar ook om de praktische toepasbaarheid ervan. Het kabinet stelde in mei 2026 dat de politie al over voldoende strafvorderlijke mogelijkheden beschikt, waaronder observatie op bevel van de officier van justitie.[68] De vraag is dan eerder waarom die mogelijkheden in het digitale domein beperkt worden benut. *Om deze knelpunten te verkleinen, zijn de volgende stappen denkbaar:*

- **Richt een permanente contentmonitor in.** Dit onderzoek laat zien dat een klein team met nieuwe testaccounts binnen enkele dagen kan vaststellen hoe snel het algoritme gebruikers naar criminele content leidt, hoe zij worden doorverwezen naar besloten kanalen en hoe een platform meldingen afhandelt. Wat nu incidenteel gebeurt, kan structureel worden ingericht. Op institutioneel niveau zou een onafhankelijke monitor gefinancierd kunnen worden die met gestandaardiseerde testaccounts periodiek meet hoe de grote platformen presteren. Zulke algoritme-audits leveren herhaalbare, vergelijkbare metingen waardoor incidenten kunnen worden verbonden met een langetermijndiagnose.
- **Veranker kennis van subculturen bij de opsporing.** Institutioneel lopen er veel versnipperde initiatieven om tactieken en internetjargon bij te houden en te decoderen. Maar ook dit kan beter en centraler ingeregeld worden, en in sterker contact met het civiele dan wel kennisinstitutionele veld. De politie, het OM, of de Autoriteit online Terroristisch en Kinderpornografisch Materiaal (ATKM) zouden deze rol kunnen vervullen mits het initiatief ook echt een landelijke hubfunctie krijgt. Het gaat daarbij minder om technische detectie dan om het vermogen te begrijpen wat posts betekenen.
- **Regel de juridische ruimte en gebruik de data die er al is.** De grens tussen openbronnenonderzoek, langdurige persoonsgerichte monitoring en digitale infiltratie moet werkbaarder worden, met passende bevoegdheden en waarborgen, zodat rechercheurs niet

67 The Hague Centre for Strategic Studies (HCSS). (2026). *Het Com-netwerk* (HCSS Focus). HCSS.

68 Kamerstukken II 2025/26, 29 754, nr. 781.

uit onzekerheid over juridische rugdekking wegkijken van wat openbaar allang zichtbaar is. Daarnaast moet Nederland de onderzoekerstoegang die de DSA regelt actief benutten.[69] Een gefinancierd consortium van Nederlandse onderzoekers zou (structureler) toegang kunnen aanvragen tot de data achter het aanbevelingssysteem van TikTok. Dat de Commissie het belemmeren van die toegang serieus neemt, bleek uit de boete die X in december 2025 kreeg.[70]

Verantwoordelijk stellen: spreek platformen aan op hun rol in de verspreiding van criminele content. Hier ligt een zwaar knelpunt. Met de Digital Services Act beschikt de EU over aanzienlijke bevoegdheden, waaronder boetes tot 6 procent van de wereldwijde jaaromzet.[71] Het afdwingen van veranderingen verloopt echter stroperig. De Europese Commissie stelde in februari 2026 voorlopig vast dat TikTok met zijn verslavende ontwerp de DSA schendt, en volgde in juli 2026 met voorlopige bevindingen over de bescherming van minderjarigen.[72] Definitieve besluiten tegen TikTok bleven tot nu toe uit. Elders wordt wel gehandhaafd: X kreeg in december 2025 een boete van €120 miljoen, Temu in mei 2026 een boete van €200 miljoen en AliExpress in juli 2026 een boete van €550 miljoen.[73] Die besluiten betroffen echter transparantie en illegale producten, niet criminele werving of algoritmische verspreiding van mogelijk schadelijke content. Dit laatste ligt juridisch ingewikkelder.

In de Verenigde Staten ontbreekt een vergelijkbaar toezichtkader, maar worden platformen via afzonderlijke rechtszaken met succes aangeklaagd. In maart 2026 legde een jury in New Mexico Meta $375 miljoen aan civiele boetes op wegens het onvoldoende beschermen van kinderen, en een dag later oordeelde een jury in Los Angeles dat Meta en YouTube aansprakelijk zijn voor schade door verslavend ontwerp van hun platform.[74] Eerder legde de Federal Trade Commission Facebook al een boete van $5 miljard op wegens privacyschendingen.[75] Het Verenigd Koninkrijk handhaaft sinds maart 2025 de illegal harms duties uit de Online Safety Act, met boetes tot 18 miljoen pond of 10 procent van de wereldwijde omzet.[76] Het Europese stelsel is in opzet het meest omvattend, maar oefent tot nu toe relatief weinig directe financiële druk uit op niet-Europese techbedrijven. *Mogelijke stappen zijn:*

- **Dien een formeel handhavingsverzoek in.** Een landelijke digitaledienstencoördinator kan de Europese Commissie via de Europese raad voor digitale diensten verzoeken een vermoedelijke inbreuk door een zeer groot platform te onderzoeken.[77] De ACM kan een dergelijk verzoek indienen, onderbouwd met herhaalbare metingen zoals beschreven onder *verkennen*. Daarnaast kan Nederland er in Europees verband op aandringen

69 Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten (digitaledienstenverordening), *PbEU* 2022, L 277, art. 40.

70 Europese Commissie. (2025a, 5 december). Persbericht over het besluit tot niet-naleving en de boete van €120 miljoen voor X onder de Digital Services Act.

71 Verordening (EU) 2022/2065, art. 74.

72 Europese Commissie. (2026a, 6 februari). *Commission preliminarily finds TikTok's addictive design in breach of the Digital Services Act* (persbericht); Europese Commissie. (2026d, 24 juli). *Commission preliminary finds TikTok in breach of Digital Services Act for failing to ensure safe accounts for minors* (persbericht).

73 Europese Commissie (2025a); Europese Commissie. (2026b, 28 mei). *Commission fines Temu €200 million for breaching the Digital Services Act*; Europese Commissie. (2026c, 20 juli). *Commission fines AliExpress €550 million for breaching the Digital Services Act*.

74 Lee, M. (2026, 24 maart). New Mexico jury says Meta harms children's mental health and safety, violating state law. *Associated Press*; Schulze, E., & Leib, M. (2026, 25 maart). Jury finds Meta, YouTube negligent in social media addiction trial. *ABC News*.

75 Federal Trade Commission. (2019, 24 juli). *FTC imposes $5 billion penalty and sweeping new privacy restrictions on Facebook* (persbericht).

76 Kennedys Law LLP. (2025). *UK Online Safety Act: How to comply as illegal harms duties take effect*.

77 Verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten (digitaledienstenverordening), *PbEU* 2022, L 277, art. 65.

de criminele werving en de handel in verboden goederen expliciet mee te wegen in de lopende procedure tegen TikTok, die nu vooral draait om haar verslavend ontwerp en minderjarigen.

- **Eis (meer) Nederlandstalige moderatie.** Uit eigen opgave van TikTok blijkt dat het aantal moderatoren voor het Nederlands daalde van ongeveer 162 in 2023 naar 45 in de eerste helft van 2026, terwijl het totale aantal EU-moderatoren in diezelfde periode met ruim 40 procent kromp.[78] In het algemeen wordt moderatie steeds verder geautomatiseerd.[79] Nederland kan eisen dat TikTok voldoende Nederlandstalige moderatie en gerichte detectie van criminele werving en normalisering opneemt in zijn risicobeperkende maatregelen, en daarover per kwartaal openbaar rapporteert.
- **Wijs betrouwbare "flaggers" aan voor criminele content.** Hoewel React zich bezighoudt met nepproducten en inbreuk op intellectueel eigendom, ontbreekt in wezen een trusted flagger die zich richt op content die geweld of drugscriminaliteit verheerlijkt, of op online werving voor criminaliteit.[80] Een gespecialiseerd team of een onafhankelijke stichting zou die status kunnen aanvragen, zodat meldingen van criminele werving minder kans lopen in de moderatiewachtrij te stranden.
- **Zet termijnen.** In december 2025 accepteerde de Commissie bindende toezeggingen van TikTok over advertentietransparantie.[81] Maar de onderzoeken naar verslavend ontwerp en de bescherming van minderjarigen lopen sinds februari 2024 en staan nog altijd in de fase van voorlopige bevindingen. Nederland kan in Europees verband aandringen op definitieve besluiten en op het daadwerkelijk benutten van de boeteruimte. De Amerikaanse praktijk laat zien dat financiële aansprakelijkheid platformen wel degelijk in beweging brengt. Ook het civiele spoor verdient steun: openbare, belastende onderzoeksresultaten moeten helpen om platformen onder druk te zetten om meer te doen.
- **Koppel meer zorgplichtverwachtingen aan een leeftijdscheck.** Het kabinet wil naar een handhaafbare Europese minimumleeftijd van 15 jaar voor sociale media. Een juridische verkenning wijst erop dat zo'n grens mogelijk is, maar dat handhaving lastig blijft.[82] Verbind aan die leeftijdsgrens concrete eisen die verder gaan dan een leeftijdscheck, zodat de oplossingslast bij het platform zelf komt te liggen. Vraag platformen aan te tonen hoe zij criminele content uit de feed van jongeren weren. Alleen een platform dat aantoonbaar veilig is, mag dan jongere gebruikers bedienen. Zo krijgt de leeftijdsgrens meer gewicht dan een symbolisch verbod en hebben platformen er zelf belang bij hun aanbod op te schonen.

78 Euronews. (2024a, 25 oktober). TikTok rolls out more European content oversight but lacks Maltese and Irish experts. *Euronews*; Euronews. (2024b, 20 november). Dutch ministry to investigate best practice for online platform content moderation. *Euronews*; TikTok. (2026b, 31 augustus). *DSA transparency report: January–June 2026*. TikTok.

79 In april-juni van 2026 nam TikTok ruim 361 miljoen moderatiemaatregelen over video's volledig automatisch, tegenover 15 miljoen met menselijke tussenkomst. TikTok. (2026c). *Community guidelines enforcement report: April–June 2026*. TikTok Transparency Center.

80 De DSA sluit publieke instanties, zoals internetverwijzingseenheden van politiediensten, daarbij uitdrukkelijk niet uit. Verordening (EU) 2022/2065, overweging 61 en art. 22.

81 Europese Commissie. (2025b). *Commission accepts TikTok's commitments on advertising transparency under the Digital Services Act* (persbericht).

82 Leerssen, P., & Van Hoboken, J. (2026, 18 juni). *Juridische verkenning naar een minimumleeftijd voor sociale media*. Instituut voor Informatierecht, Universiteit van Amsterdam.

TikTok volledig blokkeren: een uiterste handhavingsinstrument?

Een volledige blokkade van TikTok is technisch denkbaar en juridisch niet categorisch uitgesloten. De Digital Services Act biedt als uiterste middel de mogelijkheid om de toegang tot een platform tijdelijk te beperken (art. 51 lid 3). Daarvoor gelden echter zware voorwaarden: eerdere handhavingsmogelijkheden moeten zijn uitgeput, de overtreding moet voortduren en ernstige schade veroorzaken, en de procedure vereist onder meer een strafbaar feit dat het leven of de veiligheid van personen bedreigt. Bovendien is rechterlijke tussenkomst noodzakelijk. Een algemene politieke wens om TikTok te verbieden is dus onvoldoende.

Een leerzaam precedent is Albanië, dat TikTok in maart 2025 voor een jaar blokkeerde na de dood van een tiener, die door de regering in verband werd gebracht met online conflicten. De regering hief de blokkade op in februari 2026, waarna het Albanese Constitutionele Hof op 11 maart 2026 oordeelde dat het verbod de vrijheid van meningsuiting en van de pers schond. De regering had volgens het Hof niet aangetoond dat een algehele blokkade het enige effectieve en noodzakelijke middel was. Bovendien bleef TikTok in de praktijk in gebruik, onder meer via VPN-verbindingen.

Voor de Europese aanpak zijn meerdere escalatieniveaus mogelijk: het afdwingen van concrete aanpassingen in aanbevelingsalgoritmen, leeftijdsbescherming en moderatie; vervolgens financiële sancties; en uiteindelijk een tijdelijke toegangsbeperking. Belangrijker dan de vraag of TikTok op zwart kan, is of een geloofwaardige dreiging met vergaande sancties platformen eerder tot structurele veranderingen kan bewegen. Een algehele blokkade heeft bovendien als nadeel dat criminele netwerken naar andere platformen kunnen migreren, terwijl ook rechtmatig gebruik wordt geraakt.

Voorkomen: preventie criminele aanwas en slachtofferschap, in het bijzonder onder jongeren. Preventie wordt bemoeilijkt doordat traditionele instituties, zoals scholen, jeugdzorg en jongerenwerk, beperkt zicht hebben op de digitale leefwereld van jongeren. Criminele socialisatie verloopt bovendien vaak subtiel, via bestaande fysieke netwerken, buitenschoolse entertainment, influencers en beloften van snel geld. Preventieprogramma's sluiten niet vanzelfsprekend aan op deze mechanismen, en hun effectiviteit is moeilijk vast te stellen. Daar komt bij dat de routes naar criminele content per interesse verschillen (paragraaf 3.2), terwijl preventie de 'online jongere' vaak als één groep benadert. Daardoor bestaat het risico dat preventie pas op gang komt wanneer jongeren al in criminele netwerken zijn opgenomen. *Hier zijn de volgende stappen denkbaar:*

- **Zet hulp in de zoekbalk.** Voor extremistische content werken platforms al met een methode waarbij gebruikers die naar zulke content zoeken, worden doorverwezen naar hulp.[83] Diezelfde aanpak is denkbaar voor criminele werving. Wie op TikTok zoekt naar 'snel geld', 'klusje' of bekende codewoorden voor nepgeld, drugs of wapens, kan een verwijzing krijgen naar voorlichting en hulp. Daarnaast verdient tegengeluid een plek in de

[83] Kamerstukken II 2025/26, 29 754, nr. 774 (Voortgangsbrief Versterkte Aanpak Online inzake extremistische en terroristische content, 17 december 2025).

feed zelf. Ondersteun clubs van jongerenwerkers en ex-gedetineerden die contranarratieven maken en de belofte van snel geld ontkrachten.

- **Maak criminele werving onderdeel van digitale geletterdheid.** Maak ook criminele content onderdeel van digitale geletterdheidsprogramma's. Bijvoorbeeld door heling, werving en money schemes herkenbaar te maken, inclusief de bijbehorende taal en visuele markers. Vergeet niet ouders en ook docenten dezelfde geletterdheid aan te reiken zodat ze er ook zinnig over kunnen opvoeden of onderwijzen.
- **Richt preventie op de risicoroutes.** Preventie is vaak ook nog gestoeld op de bekende risicogroepen, bijvoorbeeld in de wijkaanpak of de persoonsgebonden aanpak. Interventies moeten zich ook toespitsen op de minder voor de hand liggende routes en actoren, zoals makers van sommige typen fraude- en money flipping-content waarbij daders of dadergroepen soms nog helemaal niet scherp in beeld zijn.

Verstoren: doorbreek criminele processen, van content en accounts tot netwerken en verdienmodellen. Het verwijderen van content of accounts betekent niet dat het achterliggende criminele proces wordt doorbroken. Netwerken wijken eenvoudig uit naar andere platforms, openen nieuwe accounts of gebruiken besloten kanalen. Hoofdstuk 4 liet zien dat de doorverwijzingen naar Telegram en Snapchat die functie vervullen. *Dat vraagt om de volgende stappen:*

- **Richt de inzet op doorverwijzingen.** Het verwijderen van één video verandert weinig zolang het account, de linkpagina en het Telegramkanaal erachter blijven bestaan. De operationele inzet moet zich richten op de keten. Een verwijzing in een bio naar een kanaal met drugsaanbod geldt als handel en is volgens TikToks eigen regels verboden. Zulke accounts moeten volledig worden verwijderd en hun bestemmingen actief worden gemeld bij het platform waar ze naartoe leiden.
- **Verbreed de bestuurlijke doorzettingsmacht.** De ATKM kan platforms bevelen terroristische content binnen een uur te verwijderen.[84] Voor openlijke criminele werving of expliciet crimineel gedrag bestaat zo'n instrument niet. Het mandaat van de ATKM, of van een vergelijkbare autoriteit, zou kunnen worden verbreed naar duidelijk afgebakende categorieën die duidelijk strafbaar zijn en via versnelde procedures kunnen worden aangepakt.
- **Bouw verder aan GRIMM.** Europols Operational Taskforce GRIMM, in april 2025 opgericht onder Zweedse leiding en met Nederlandse deelname, richt zich op *violence-as-a-service*, inclusief digitale rekrutering, de verdienmodellen erachter en internationale dadersamenwerking. In het eerste jaar leidde dat tot 280 aanhoudingen.[85] Waar dat eventueel nog niet gebeurt, kan Nederland de taskforce voeden met platformsignalen uit eigen monitoring.

Vervolgen: intensiveer grensoverschrijdende vervolging en focus opsporing op de werver. Digitale criminaliteit is veelal grensoverschrijdend, terwijl opsporing en vervolging gebonden blijven aan nationale rechtsstelsels. Vluchtige chatgegevens en anonieme accounts bemoeilijken de bewijsvergaring. Bovendien vervagen bij online rekrutering de grenzen tussen daderschap en slachtofferschap. Dat compliceert zowel de strafrechtelijke beoordeling als de keuze tussen repressieve en zorggerichte interventies. *Een van de stappen die denkbaar is:*

---

84 *Evaluatie Uitvoeringswet verordening terroristische online inhoud* (2026).

85 Schrader, M., & Linssen, F. (2026, 28 april). Europol: 280 verdachten opgepakt voor ronselen jongeren voor 'geweld op bestelling'. *NOS*.

- **Richt de strafrechtelijke druk op de werver, niet op de uitvoerder.** De minister van Justitie en Veiligheid acht het huidige instrumentarium voldoende om ronselaars aan te pakken.[86] Toch vroeg de Tweede Kamer in september 2026 om meer inzicht in de werkwijze van online ronselaars en hun strafvervolging.[87] Een in mei 2026 ingediend amendement beoogt een strafverzwaring voor het werven van minderjarigen voor drugsdelicten.[88] Die gedachte is goed maar verdient een bredere uitwerking. Men denke aan een algemene strafverzwaringsgrond voor het werven van minderjarigen, ongeacht het delict. Tegelijk moet de minderjarige soms als mogelijk slachtoffer worden benaderd. Bijgevolg moet ook de strafrechtelijke aanpak op dit gegeven ingericht zijn.

Dit alles vraagt om een strategische agenda voor meerdere jaren, niet om politieke losse flodders. Omdat niet alles tegelijk kan, moet men nu prioriteren daar waar de hefboomeffecten het grootst zijn en daar consequent op blijven inzetten, zowel nationaal als Europees. Pas wanneer het voor platformen meer kost om weg te kijken dan om op te treden, ontstaat er werkelijke verandering. Zonder drukmiddelen blijft het dossier fundamenteel onoplosbaar.

86 Minister van Justitie en Veiligheid. (2026, 26 maart). *Antwoorden op Kamervragen van de leden Schilder en Moinat over het bericht 'Jongeren vatbaar voor 'snel geld''* (2026Z01964).

87 Kamerstukken II 2025/26, 29 911, nr. 522 (motie Schilder).

88 Kamerstukken II 2025/26, 36 705, nr. 8 (amendement Faber).

6. Conclusie

Deze HCSS Focus begon met een maatschappelijke intuïtie: dat socialemediaplatformen bijdragen aan een sfeer van digitale normloosheid, waarin criminele content eerder norm dan uitzondering wordt. Op basis van het verkennende OSINT-onderzoek op TikTok is die intuïtie in de kern terecht.

Belangrijkste vaststellingen. Criminele content is op TikTok openlijk en zonder noemenswaardige drempel beschikbaar, verspreid over meerdere contenttypen. Het algoritme reikt deze content bovendien actief aan, ook aan wie er niet naar zoekt. Ook fungeert TikTok als doorzetportaal. Bijna de helft van de onderzochte accounts met criminele content verwees door naar andere kanalen. Op basis van onze verkennende bevindingen schiet ook het vangnet tekort. Van honderd gemelde posts die de richtlijnen van TikTok lijken te schenden, bleek maar een fractie verwijderd.

Maatschappelijke implicaties. Sociale media zijn waarschijnlijk niet de voornaamste ingang tot daadwerkelijke criminaliteit. Het eigen netwerk van familie, buurt en school blijft van belang, en online contact haakt daar eventueel op aan. De grootste maatschappelijke betekenis van deze bevindingen ligt in normalisering. Wanneer een algoritme jongeren dagelijks voorziet van verhalen in de trant van een criminele statuseconomie, verschuift het referentiekader. Met hun aanbevelingssystemen bepalen platformen in hoge mate wat jongeren te zien krijgen, en daarmee wat zij als normaal gaan beschouwen.

Strategische aanknopingspunten. De aanpak schiet op dit moment vooral tekort in uitvoering, consequente handhaving, en politieke drukuitoefening, niet zozeer in kaders. Er is regelgeving, er zijn bevoegdheden en er zijn programma's, maar het zicht op wat er online gebeurt is versnipperd en de handhaving richting platformen is traag.

Onze strategische richtpunten kunnen worden samengevat langs drie algemenere blikverschuivingen.

- Beweeg van incidentele signaleringen naar systematische prestatiemonitoring. Een permanente, onafhankelijke monitor kan systematisch meten hoe snel jongeren bij criminele content uitkomen en hoe platformen meldingen afhandelen.

- Beweeg van vrijblijvende samenwerking naar meer afdwingbaarheid. Nederland kan formele handhavingsverzoeken bij de Europese Commissie indienen, Nederlandstalige moderatie eisen, "flaggers" voor criminele content aanwijzen, enz.; en zo uiteindelijk meer druk organiseren.

- Beweeg van de focus op individuele gevallen naar de vernetwerkte exploitatiesystematiek. Verstoring en opsporing moeten zich richten op de doorverwijzingsstructuren en achterliggende wervingsnetwerken.

Het algoritme dat jongeren ook naar nadrukkelijk schadelijke content leidt, is in de basis altijd al een ontwerpkeuze geweest die we met de massale omarming van socialemediabedrijven hebben gedoogd. De logische effecten van socialemediaconsumptie, de verleiding en de normalisering van malafide content waren in die zin te voorzien. Nu ligt er een verantwoordelijkheid om de excessieve gevolgen terug te dringen ondanks de macht en positie die platformen in onze levens hebben verworven. De kern van de opgave is om die maatschappelijke urgentie om te zetten in doortastender optreden tegenover het aandachtsmodel van socialemediaplatformen.



The Hague Centre
for Strategic Studies

HCSS
Lange Voorhout 1
2514 EA The Hague

Follow us on social media:
@hcssnl

The Hague Centre for Strategic Studies
Email: info@hcss.nl
Website: www.hcss.nl