Internationaal en Europees strafrecht en Mensenrechten / International and European Criminal Law, and Human Rights Law

Strafrecht en de informatiemaatschappij

Gert Vermeulen[a]

a Belgisch rapporteur voor Sectie IV, voorzitter Belgisch-Luxemburgse Unie voor Strafrecht (BLUS); directeur-generaal publicaties en lid bestuurscomité, directiecomité en wetenschappelijk comité AIDP; Hoogleraar internationaal en Europees strafrecht, Institute for International Research on Criminal Policy (IRCP), Universiteit Gent (Corresp.: Gert.Vermeulen@UGent.be); Bijzonder Hoogleraar Evidence, Universiteit Maastricht (Corresp.: g.vermeulen@maastrichtuniversity.nl).

In Panopticon nr. 2014.6 verscheen reeds een kort verslag (van de hand van Els De Busser) over het 19de vijfjaarlijkse congres van de *Association Internationale de Droit Pénal* (AIDP), dat van 31 augustus tot 6 september 2014 werd gehouden in Rio de Janeiro, Brazilië.

Naar traditie publiceren we in deze rubriek ook een officieuze Nederlandse vertaling van de resoluties (officieel enkel aangenomen in het Engels, Frans en Spaans) van de vier secties van het congres, die respectievelijk handelen over algemene beginselen van strafrecht (I), bijzonder strafrecht (II), strafprocedure (III) en internationaal strafrecht (IV). De preambules van de sectieresoluties zijn hieronder niet mee opgenomen.

Het overkoepelende congresthema en dus tegelijk de rode draad doorheen de secties was: de informatiemaatschappij en strafrecht.

Sectie I | Algemene beginselen van strafrecht

A. Algemene bemerkingen voor strafwetgeving

1. ICT-netwerken en cyberspace hebben specifieke belangen gecreëerd die gerespecteerd en beschermd dienen te worden, bijvoorbeeld privacy van individuen, vertrouwelijkheid, integriteit en beschikbaarheid van ICT-netwerken, en integriteit van persoonlijke identiteiten in cyberspace. Daders van bepaalde traditionele misdrijven, bijvoorbeeld fraude, valsheid in geschrifte en inbreuken op het auteursrecht (copyright) maken gebruik van ICT-netwerken en cyberspace, waardoor de gevaarlijkheid van hun gedrag vergroot. Wetgevers, rechtbanken en strafrechtssystemen dienen de uitdaging te aanvaarden zich voortdurend aan deze situatie aan te passen.

2. Omdat vertrouwelijkheid, integriteit en beschikbaarheid van ICT-netwerken en cyberspace vitaal zijn voor individuen, alsook voor de media, en schadelijk of gevaarlijk gedrag in deze domeinen belangrijke belangen kan raken, dienen staten en internationale organisaties het bedenken van effectieve beleidslijnen met betrekking tot de bescherming van ICT-netwerken en de getroffen belangen voort te zetten. Dergelijke beleidslijnen dienen de mensenrechten te beschermen en conform te zijn met de basisbeginselen van strafwetgeving, met inbegrip van het proportionaliteitsbeginsel. Zij dienen continu bijgewerkt te worden met oog op het vermijden van nieuwe vormen van schadelijk of gevaarlijk gedrag. Empirisch en technisch onderzoek dient aangemoedigd en gefinancierd te worden om wetgevers in deze domeinen bij te staan.

3. Anderzijds dienen excessieve regulering en criminalisering van cyberspace vermeden te worden, aangezien het de vrijheid van communicatie, die de cyberspace net karakteriseert, in gevaar brengt. Wetgevers dienen ervan bewust te zijn dat de regulering van gedrag, de

totstandbrenging van strafwetten en de oplegging van disproportioneel restrictieve controlemaatregelen in cyberspace in aanvaring kan komen met de mensenrechten, in het bijzonder de vrijheid van meningsuiting en de vrijheid om informatie te ontvangen, te verwerken en te verspreiden.

4. Wetgevers dienen geen gedrag te criminaliseren dat enkel religieuze of morele normen schendt. Strafrechtelijk beleid dient consistent te zijn met het schadebeginsel. Bijgevolg dienen wetgevers geen gedrag te criminaliseren dat niet schaadt of een concreet gevaar creëert voor enig belang van een persoon of een collectief belang, met inbegrip van de vertrouwelijkheid, integriteit en beschikbaarheid van ICT-netwerken.

B. Preventie van misdrijven en alternatieven voor strafrechtelijke bestraffing

5. Gebruikers van ICT-netwerken en systeemproviders dienen aangespoord te worden om de veiligheid van netwerken te beschermen, met inbegrip van zelfregulering door providers. Het niet naleven van dergelijke veiligheidsmaatregelen kan niet leiden tot strafrechtelijke aansprakelijkheid aan de zijde van de gebruikers. De wetgevers kunnen evenwel de inbreuk op specifieke verplichtingen strafbaar stellen om zo de veiligheid van de gegevens van andere personen te verzekeren.

6. Indien noodzakelijk voor preventiedoeleinden, kunnen wetgevers toelaten om, in overeenstemming met het proportionaliteitsbeginsel, gegevens op te slaan die mogelijk maken om, onder effectief gerechtelijk toezicht, gebruikers te identificeren.

7. Aangezien strafrechtelijke verbodsbepalingen sterke morele afkeuring teweegbrengen en daders kunnen stigmatiseren, dienen staten grondig te onderzoeken of niet-strafrechtelijke maatregelen even effectief kunnen zijn om aanvallen op ICT-netwerken en misbruiken van cyberspace te vermijden. Rechterlijke bevelen en het herstel van de schade toegebracht aan de slachtoffers conform het burgerlijk recht, evenals maatregelen van herstelrecht, kunnen goede alternatieven vormen voor strafrechtelijke sanctionering. Administratieve maatregelen, zoals het ontzeggen van toegang tot illegaal materiaal of het weghalen van dergelijk materiaal van websites, kan ook een voldoende preventief effect teweegbrengen en het gebruik van strafwetgeving overbodig maken. Administratieve maatregelen kunnen evenwel niet disproportioneel zijn of omslaan in censuurpraktijken uitgevoerd door uitvoerende instanties.

C. Omschrijving van strafbare feiten

8. In overeenstemming met het legaliteitsbeginsel, dienen wetgevers strafbare feiten met betrekking tot ICT zo nauwkeurig mogelijk in functionele termen te omschrijven. Wanneer technologie wijzigt, dient de wet mogelijk gewijzigd te worden. Het legaliteitsbeginsel is ook van toepassing op de omschrijving van de taken en verplichtingen van natuurlijke en rechtspersonen, in zoverre dat een inbreuk hierop kan leiden tot strafrechtelijke verantwoordelijkheid. Rechtbanken dienen het toepassingsgebied van statutaire strafrechtelijke verbodsbepalingen niet verder te verruimen dan hun letterlijke betekenis.

D. Uitbreiding van strafwetten

9.De strafbaarstelling van de loutere voorbereiding van aanvallen op ICT-netwerken en cyberspace, zoals de productie, de distributie en het bezit van malware, is enkel legitiem voor zover deze voorbereidende handelingen op zich schade veroorzaken of concreet gevaar creeren voor de beschermde belangen van anderen of de vertrouwelijkheid, integriteit en beschikbaarheid van ICT-netwerken. Wanneer voorbereidende handelingen strafbaar worden gesteld, dient de straf minder zwaar te zijn dan de straf voor het voltooide strafbare feit (zie in dit verband de resoluties van het XVIIIde Internationaal Strafrechtscongres in Istanbul 2009, Sectie I (A)).

10. Het bezit van software dient niet gecriminaliseerd te worden louter en alleen om het bewijs van wandaden te vergemakkelijken. Dergelijke criminalisering dient het legitiem gebruik van software niet al te zeer te beperken.

11. Het louter bezitten en bekijken van gegevens kan enkel strafbaar gesteld worden wanneer bezit en bekijken intentioneel is en rechtstreekse of onrechtstreekse schade of concreet gevaar teweegbrengen voor beschermde belangen.

12.

a) Internet access providers kunnen niet strafrechtelijk verantwoordelijk gesteld worden indien ze nalaten controle uit te oefenen op de inhoud die zij verwerken.
b) Strafrechtelijke verantwoordelijkheid van host service providers dient beperkt te worden tot de gevallen waarin:

    - ze specifiek door de wet verplicht worden om bepaalde inhoud te controleren vooraleer ze beschikbaar gemaakt wordt voor gebruikers, het voor hen redelijkerwijze haalbaar is dit te doen, en ze bewust verzuimen om deze verplichting na te komen, of
    - ze op een betrouwbare en specifieke wijze gewezen waren op het feit dat ze illegale inhoud beschikbaar stellen, en bewust verzuimen om prompt alle redelijke maatregelen te nemen om die inhoud onbeschikbaar te maken.

E. Internationale harmonisatie van wetten

13. Beleidslijnen voor de bescherming van ICT-netwerken en cyberspace en de belangen van gebruikers dienen wereldwijd geharmoniseerd te worden om ernstige discrepanties tussen reguleringen van dezelfde materie te vermijden, om internationale samenwerking te verbeteren, en om bevoegdheidsconflicten te vermijden.

Sectie II | Bijzonder strafrecht

1. Bij de aanpak van de dreiging en realiteit van cybercriminaliteit en de noodzaak van cyberveiligheid, dienen het rechtssysteem en het strafrechtssysteem een afweging te maken tussen individuele en collectieve belangen, belangen van de private sector en de overheid. Een overdreven vertrouwen op strafrechtelijke bescherming dient vermeden te worden ten gunste van sterke preventie, actieve verdediging, voorlichting en bewustwording van de bevolking, en alternatieve sancties.

2. De juridische belangen die dienen beschermd te worden, omvatten onder meer de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en ICT-systemen, authenticiteit van informatie, leven, integriteit van kinderen, privacy, bescherming tegen beschadiging aan en verlies van eigendom (inclusief virtueel eigendom), auteursrecht (copyright) en reputatie, vrijheid van meningsuiting, en andere fundamentele mensenrechten.

3. Consumentenbescherming, geïnformeerde toestemming, doelbinding, het recht om vergeten te worden, op verbetering en op mededeling, zullen de voornaamste belangen zijn bij het richting geven aan de verwoording van de wetten en voorschriften over gegevensverzameling, verkopen en aankopen op het internet, financiële transacties en investeringen, en marketing- en promotiecampagnes.

4. Commerciële verwerkers van persoonsgegevens, zoals internet en telecomproviders, social media platforms, en application developers, dienen verplicht te worden om beleidsmaatregelen met betrekking tot privacy by design en privacy by default aan te nemen, indien nodig door dwangmaatregelen. De schending hiervan dient bestraft te worden met niet-strafrechtelijke of strafrechtelijke sancties.

5. Een gezamenlijke inspanning is essentieel om illegale toegang tot ICT-systemen te voorkomen en te bestrijden; de illegale onderschepping van niet-publieke overdrachten van elektronische gegevens; onrechtmatige inmenging in gegevens en systemen; het misbruik van toestellen, software, paswoorden, en codes; computergerelateerde namaak en fraude; en ongeoorloofde toegang door overheidsinstellingen. Dit behelst een minimale standaard van strafrechtelijke bescherming tegen intentionele en schadelijke handelingen die de vertrouwelijkheid, integriteit en toegankelijkheid van gegevens en van ICT-systemen schenden.

6. Er is nood aan geschikte wettelijke maatregelen om verzwarende omstandigheden of specifieke misdrijven van strengere sancties te voorzien bij inmenging in de werking van cruciale informatie- en communicatiestructuren.

7. De productie en de bewuste distributie, verspreiding, import, export, aanbod, verkoop, aankoop, bezit, en verkrijgen van kinderpornografie en elke medeplichtigheid en deelname aan een van deze handelingen zal krachtig en consistent vermeden en strafbaar gesteld worden met gepaste sancties, in het bijzonder wanneer echte kinderen betrokken zijn, tenzij voor eigen privaat gebruik wanneer ze de leeftijd van seksuele meerderjarigheid bereikt hebben.

8. Gehele of gedeeltelijke identiteitsdiefstal, inclusief door phishing, dient strafbaar gesteld te worden, indien dit niet anders bepaald is in andere strafrechtelijke bepalingen. Indien Staten ervoor opteren het loutere bezit van identiteit gerelateerde informatie of zich uitgeven voor niet-bestaande personen strafbaar te stellen, dient dit beperkt te blijven tot handelingen gepleegd met het opzet om schade te veroorzaken. Dergelijke bepalingen kunnen in geen geval de vrijheid van denken en van meningsuiting, en in het bijzonder literaire en artistieke activiteiten, beperken of strafbaar stellen.

9. Gelet op de toenemende bezorgdheid over de frequentie en de ernst van cyber stalking, cyber bullying, en cyber grooming, dient hieraan bijzondere aandacht geschonken te worden om doeltreffend op het probleem te kunnen antwoorden, waarbij positieve benaderingen,

preventie, algemene bewustwording en voorlichting, en alternatieve sancties de voorkeur genieten boven de loutere toepassing van strafrechtelijke bescherming.

10. De bescherming van intellectuele eigendomsrechten dient zich toe te spitsen op opzettelijke schendingen die een beduidend commercieel doel hebben of serieuze schade voortbrengen.

11. Roekeloos of grof nalatig beheer van cruciale ICT-infrastructuur en van grote hoeveelheden gevoelige gegevens, zoals kredietkaartgegevens, dienen hersteld te worden door niet-strafrechtelijke of strafrechtelijke sancties. In dezelfde zin kan het verzuim redelijke veiligheidsmaatregelen aan te nemen en/of tijdig de vereiste informatie te verschaffen over inbreuken op de beveiliging door internet service providers een reden zijn voor burgerlijke of strafrechtelijke gevolgen.

Sectie III | Strafprocedure

A. Het gebruik van ICT en de bescherming van de mensenrechten

Het gebruik van ICT in strafrechtelijke procedures en in de uitbouw van informatieposities kan een substantiële inbreuk vormen op de fundamentele rechten. De volgende principes moeten in het bijzonder gerespecteerd worden:

1. Elke beperking op het recht op privacy zal bij wet voorzien worden en zal proportioneel, legitiem en noodzakelijk zijn in een democratische samenleving.

2. Het gebruik van ICT in strafrechtelijke procedures en in de uitbouw van informatiesystemen moet het recht op gegevensbescherming eerbiedigen. De doeleinden van criminaliteitspreventie en strafrechtelijk onderzoek moet proportioneel zijn aan de inbreuk op het fundamentele recht op databescherming.

3. Het doelbindingsbeginsel moet gerespecteerd worden, en in het bijzonder bij het verzenden van elektronische persoonlijke gegevens aan rechtshandhavingsautoriteiten. Het doelbindingsbeginsel houdt in dat persoonlijke gegevens slechts verzameld kunnen worden voor een uitdrukkelijk, bepaald en legitiem doel, en erna niet verder kunnen gebruikt worden op een manier die onverenigbaar zou zijn met deze doeleinden.

4. Een inbreuk op de doelbinding mag alleen worden toegestaan in overeenstemming met de wet, in uitzonderlijke gevallen, wanneer de overbrenging van gegevens naar rechtshandhavingsautoriteiten noodzakelijk is voor de preventie, het onderzoek of de vervolging van serieuze misdrijven en wanneer het proportionaliteitsbeginsel gerespecteerd wordt.

5. Het wettelijk kader moet verzekeren dat er adequate middelen en barrières voor de toegang en de ontsluiting van bewaarde gegevens worden ingesteld en dat zij beheerd worden door een onafhankelijk autoriteit. Als er een verplichting rust op een publiek en/of private onderneming om computergegevens bij te houden, te bewaren en te verzenden, dan moet deze het recht op databescherming respecteren.

6. Het gebruik van ICT in strafrechtelijke procedures mag de rechten van verdediging niet schenden, onder andere, het recht op een openbare zitting, op tegenverhoor en confrontatie,

op toegang tot het dossier en op bijstand van experten die gespecialiseerd zijn op het gebied van elektronische bewijsvoering om de gelijkheid van wapens te garanderen.

B. ICT-intelligence en de opbouw van informatieposities

7. De wet moet vastleggen welke maatregelen gebruikt kunnen worden door handhavingsautoriteiten voor de opbouw van informatieposities en het vastleggen van het doel, de omvang en de vereisten van deze maatregelen, met inbegrip van de voorwaarden voor de vernietiging van deze gegevens en/of de vernieling van de gegevensdrager.

8. Dwangmaatregelen zouden niet toegestaan mogen worden om gegevens te verzamelen voor de opbouw van informatieposities, tenzij bij gerechtelijk bevel. Een gerechtelijk bevel zou ook nodig moeten zijn voor de opbouw van informatieposities door non-open source data mining en/of data matching.

9.Geen enkele toezichtsmacht gebruikt voor de opbouw van informatieposities mag het recht op privacy of andere fundamentele rechten schenden.

10. Er moet gebruik gemaakt worden van geschikte technische middelen om de toegang tot gegevens te beheren. Een onafhankelijk orgaan moet de toegang tot gevoelige data beheren.

11. Een wet moet vastleggen in welke gevallen en onder welke omstandigheden gegevens, verzameld voor de opbouw van informatieposities overgebracht mogen worden naar een andere autoriteit.

C. ICT in het strafrechtelijk onderzoek

12. ICT-onderzoeksmaatregelen, zoals elektronisch toezicht, monitoren van de geolocatie, verzameling van real-time of bewaarde gegevens, geheime online onderzoeken, de inbeslagname en het doorzoeken van computergegevens, het uitgebreid doorzoeken van verbonden netwerken, bevelen voor het aanleveren of decoderen van computergegevens, toegang en/of analyse van communicatiegegevens die op mobiele toestellen wordt bewaard, het gebruik van forensische hulpmiddelen op afstand en de onderschepping van elke vorm van communicatie die uitgevoerd wordt met een strafrechtelijk onderzoek als doel zullen enkel worden toegelaten in gevallen bepaald bij wet wanneer de gewenste informatie niet bekomen kan worden door minder indringende middelen. De reikwijdte van de onderzoeksbevoegdheden, de maximale duur van de onderzoekshandeling en de vereisten voor de bewaring en/of vernietiging van de verkregen gegevens, en/of de vernieling van de gegevensdrager, moet bij wet bepaald worden.

13. ICT-onderzoeksmaatregelen die een ernstige inbreuk vormen op het recht op privacy, zoals diegene die toegang verschaffen tot de inhoud van communicatie, die de onderschepping van real-time of bewaarde gegevens met zich meebrengen, of het gebruik van onderzoeksmiddelen op afstand, moeten in de regel enkel toegestaan worden door rechterlijke machtiging en alleen in gevallen bij redelijke verdenking van het plegen van ernstige misdrijven, en als het doel verbonden is met het plegen van zulke misdrijven.

14. Personen wiens recht op privacy aangetast werd door ICT-onderzoeksmaatregelen moeten geïnformeerd worden van deze maatregelen vanaf het moment dat deze bekendmaking

het doel van de maatregel en/of de resultaten van het strafrechtelijk onderzoek niet in gevaar brengt. De wet moet effectieve juridische hulpmiddelen voorzien om de wettelijkheid van het gebruik van ICT-onderzoeksmaatregelen aan te vechten en het recht op vertrouwelijkheid beschermen.

15. Tijdens de uitvoering van ICT-onderzoeksmaatregelen die toegang verlenen tot computergegevens en elektronische communicatie moet het recht op vertrouwelijkheid en het beroepsgeheim gerespecteerd worden. De bekendmaking van gegevens die geen verband houden met de strafrechtelijke procedures, moet voorkomen worden.

16. Staten hebben een positieve verplichting om ervoor te zorgen dat de rechtshandhavingsautoriteiten over de nodige technische middelen, capaciteiten en deskundige training in het gebruik van ICT beschikken om om te gaan met geavanceerde vormen van cybercrime en elektronische informatie in het algemeen. Richtlijnen voor goede praktijken moeten worden ontwikkeld en toegepast in onderzoeken waarbij ICT gebruikt wordt.

17. De samenwerking van particuliere bedrijven en ICT-dienstverleners met rechtshandhavingsautoriteiten in het strafrechtelijk onderzoek die een inbreuk op de fundamentele rechten kan vormen, wordt bij wet geregeld. De omvang, voorwaarden en eisen voor een dergelijke samenwerking moet in de wet worden ingesteld. Naleving van dergelijke wettelijke verplichtingen mag niet leiden tot burgerlijke aansprakelijkheid van het bedrijf ten aanzien van zijn klanten.

D. Bewijs en ICT

18. Vanwege het vluchtige karakter van elektronisch bewijs moet de wet de snelle bewaring en opslag van digitale gegevens vergemakkelijken. Forensische hulpmiddelen voor de voorkoming van veranderingen van de opgeslagen gegevens moeten beschikbaar zijn en regelmatig gebruikt worden.

19. Als de betrouwbaarheid van ICT-bewijs wordt aangevochten, moet de 'bewijscontinuïteit' of 'chain-of-custody' worden vastgesteld. De verdediging moet de toegang tot de digitale gegevens worden gegarandeerd, zodat zij in staat is om de echtheid te controleren, en om het tijdens het proces voor te leggen op een effectieve en niet onnodig beperkte manier.

20. Elektronisch bewijs dat direct of indirect verkregen werd door middelen die een schending zijn van de fundamentele rechten en vrijheden die de gelijkheid van wapens en het eerlijke verloop van de procedure in gevaar brengen, zijn ontoelaatbaar.[1]

21. Rechtszalen moeten worden uitgerust voor het gebruik van ICT in de loop van het strafproces. Financiële middelen om dit doel te bereiken moet worden verstrekt.

22. Video-conferencing moet beschikbaar zijn om het getuigenis van getuigen die kwetsbaar of niet beschikbaar zijn mogelijk te maken, zodat de identiteit van de getuige beschermd kan worden en ze ondervraagd kunnen worden in de gevallen toegestaan bij wet.

[1] Voor de toelaatbaarheid van intelligence als bewijs, zie punt 22 van de resolutie die werd aangenomen op het XVIIIde Internationaal Strafrechtscongres (Istanbul, 2009) over 'Bijzondere procedurele maatregelen en respect voor de mensenrechten.'

23. Het onderzoek en de ondervraging van minderjarige slachtoffers tijdens de fase voorafgaand aan het proces moet op video opgenomen worden voor het geval dat het kind niet beschikbaar is om te getuigen tijdens het proces om redenen die verband houden met de bescherming van het welzijn van het kind.

24. De verweerder moet, in de regel, altijd fysiek aanwezig zijn tijdens een gerechtelijke procedure. In de zeldzame gevallen waarin de aanwezigheid door middel van video-conferencing is toegestaan, moet het georganiseerd worden op een manier die het recht om zichzelf niet te beschuldigen, als ook het recht op juridische bijstand (inclusief die van vertrouwelijke communicatie met een advocaat) en het recht op de ondervraging van getuigen voldoende beschermt.

Sectie IV | Internationaal strafrecht

A. Algemene beschouwingen

1. De Staten moeten een coherent antwoord bieden aan de uitdagingen van cybercriminaliteit, met name door hun wetgeving en praktijk te blijven herzien om ervoor te zorgen dat hun strafrecht, strafprocesrecht en wederzijdse rechtshulp voldoen aan de behoeften van de onderling verbonden geglobaliseerde wereld van vandaag, met eerbied voor de fundamentele en mensenrechten.

2. Staten dienen toe te treden tot de bestaande internationale instrumenten inzake cybercriminaliteit. De staten en de internationale gemeenschap moeten verdere internationale juridische mechanismen uitwerken, waaronder de nalevingsnormen voor multinationale ondernemingen, om de rechtsstaat in cyberspace te ontwikkelen en potentiële conflicten te voorkomen tussen staten over de handhaving van hun wetgeving en beleid in cyberspace.

B. Substantiële rechtsmacht en locus delicti

3. Terwijl het territorialiteitsbeginsel ook in cyberspace het belangrijkste principe blijft om de rechtsmacht te bepalen, heeft het negatieve effecten als gevolg wanneer het toegepast wordt op overtredingen in cyberspace. In die mate dat het de facto staten toelaat misdrijven op hun grondgebied te lokaliseren op een bijna universele basis en individuen in twijfel laat welke staten zich de rechtsmacht kunnen toe-eigenen. Staten moeten zich terughoudend opstellen bij de uitoefening van hun rechtsmacht in situaties waarin het effect niet in de staat is 'geduwd' door een dader, maar door een individu in die staat 'getrokken' is.

4. Bij het bepalen van gevolgen, moeten staten het bestaan van een bepaald verband met de strafbare feiten nagaan, zoals de intentie van de dader die blijkt uit het gebruik van een bepaalde taal, het aanbieden van binnenlandse betalingsfaciliteiten, een dienstenaanbod in bepaalde steden, etc.

5. Wanneer een staat de gevolgen van een overtreding binnen haar grenzen lokaliseert, vereist het legaliteitsbeginsel dat de dader een redelijke verwachting had kunnen hebben dat zijn of haar gedrag gevolgen in dat land zou veroorzaken.

6. Een staat kan zijn rechtsmacht over een persoon op zijn grondgebied uitoefenen, die content 'trekt' die onder zijn eigen rechtssysteem is verboden, ook al is het wettelijk in de rechtsorde van de producent.

7. De staten en de internationale gemeenschap moeten overwegen om nalevingsvereisten en aansprakelijkheid voor strafrechtelijke inbreuken door rechtspersonen met betrekking tot cybercrime vast te leggen.

C. Onderzoek in cyberspace

8. Geen enkele staat heeft exclusieve soevereiniteit over de ICT-netwerken die publiek toegankelijk zijn.

9. Uitgezonderd in gevallen waar dwang- of infiltratiemaatregelen worden toegepast, hebben de rechtshandhavingsautoriteiten het recht op vrije toegang tot (en het recht om vrij te werk te gaan in) de ICT-netwerken die vrij toegankelijk zijn zonder toelating van providers en/of staten, ongeacht waar de inhoud die wordt bekeken, bewaard wordt.

10. Om cybercrime te voorkomen en het onderzoek van nut te laten zijn, moeten staten en de internationale gemeenschap overwegen om verplichtingen op te leggen aan service providers, software en applicatie ontwikkelaars en andere relevante private ICT-stakeholders om gegevensbescherming, privacy vriendelijke technologie en instellingen te versterken.

11. Staten moeten overwegen om in het nationale recht een verplichting op te leggen aan service providers om samen te werken met rechtshandhavingsautoriteiten, onderworpen aan de autorisatie door een onafhankelijk rechtelijke autoriteit (bijvoorbeeld om gegevensoverdrachten in de cyberwereld opspoorbaar te maken, om toegang te krijgen tot wachtwoorden, om inhoud te ontcijferen of om zoekmiddelen voor onderzoek te installeren). Deze verplichting is onderhevig aan het proportionaliteitsbeginsel en de naleving van de fundamentele rechten en mensenrechten.

12. Staten die onderzoeken uitvoeren, moeten alle betrokken personen de bescherming aanbieden die hen zou toekomen in een soortgelijke nationale zaak. Daarnaast moeten ze ook de bescherming krijgen die hen zou toekomen onder het nationale rechtssysteem van de staat waar onderzoeksmaatregelen worden uitgevoerd of waar de betrokken personen verblijven wanneer de onderzoeksmaatregelen worden uitgevoerd.

D. Internationale samenwerking en handhaving in strafzaken

13. Staten moeten ervoor zorgen dat bij het toekennen van wederzijdse rechtshulp bij cybermisdrijven, ze alle onderzoeksmaatregelen kunnen nemen die ze wettelijk kunnen nemen in een gelijkaardige nationale zaak.

14. Staten moeten in het bijzonder in staat zijn om snel hulp te bieden en om voorlopige maatregelen te bevelen om informatie en bewijs te bewaren of te bevriezen gedurende een redelijke tijd en zonder onnodig in te grijpen op de rechten van de partijen.

15. Staten mogen geen wederzijdse rechtshulp weigeren op basis van het ontbreken van een dubbele incriminatie voor cybercrimemisdrijven wanneer de strafbaarheid is vereist op basis van een internationaalrechtelijke verplichting die op hen rust.

16. Een (voorlopige) beslissing, door een onafhankelijke rechterlijke instantie, om een server of website af te sluiten of een aanvraag van een staat om botnet af te sluiten, kan rechtstreeks worden afgedwongen indien daarin wordt voorzien door een internationale overeenkomst of door het recht van de staat waarin de dienstverlener of het botnet command en control-server zich bevinden. Waar mogelijk moet de voorkeur worden gegeven om de website enkel ontoegankelijk te maken op het grondgebied de verzoekende staat alleen, waardoor onnodige beperking van de cybervrijheid wordt vermeden.

17. Het latere gebruik van informatie die door de inlichtingendiensten in strafzaken is verzameld, wordt alleen toegestaan indien de betrokken informatie had kunnen worden verkregen door middel van regelmatige mechanismen voor samenwerking in strafzaken op juridisch.

E. Effectieve mensenrechten in een virtuele wereld

18. Staten moeten de internationaal erkende fundamentele rechten en mensenrechten die van toepassing op hen zijn ook in de context van de digitale wereld respecteren.

19. Als staten een extraterritoriale handeling uitvoeren bij onderzoek in cyberspace, moeten deze in overeenstemming zijn met de normen van de mensenrechten die van toepassing zijn op hun rechtsmacht (agent control standard), alsook met de diegene die van toepassing zijn op de staat waar het extraterritoriaal onderzoek plaatsheeft en wanneer de betrokken personen zich bevinden wanneer het extraterritoriaal onderzoek plaatsheeft.

20. Staten moeten onderzoek in cyberspace registreren met het oog op het waarborgen van de verantwoordelijkheid van de staat bij het voorkomen van schendingen van de fundamentele rechten en mensenrechten. Ze moeten deze opnames ook ter beschikking stellen van de verdediging om een eerlijk proces te waarborgen en bij het instellen van een rechtsmiddel bij de controlemechanismes.

21. Bij schendingen van de fundamentele rechten en vrijheden kan de verantwoordelijkheid van een bepaalde staat pas vaststaan na de vaststelling van de schending en mag deze niet als een voorwaarde voor de ontvankelijkheid van een klacht bij controlemechanismes beschouwd worden.

F. Virtuele rechtszaal

22. Communicatie mag digitaal verzonden worden door de autoriteiten, rechtstreeks aan de verdachten, de beschuldigden, de getuigen, de slachtoffers en de experten die fysiek aanwezig zijn in een andere staat op voorwaarde van hun toestemming voor deze communicatiemethode. Een vertaling dient bij de communicatie gevoegd te worden, in een taal die door de bestemmeling begrepen wordt, alsook een vermelding van de rechten en plichten van de bestemmeling met betrekking tot de ontvangen communicatie, in het bijzonder het recht op bijstand, de verschijningsplicht en meineed.

23. De mogelijkheden om gebruik te maken van digitale technologie, zoals videolinks, moet in internationale strafzaken uitgebreid worden om de nood aan dwangmaatregelen zoals uitlevering te verminderen en om de onnodige tijdelijke overbrenging van gedetineerden, de fysieke verschijning van getuigen en experts voor buitenlandse autoriteiten te verminderen.

24. Staten moeten aangemoedigd worden om de mogelijkheid en de voorwaarden na te gaan van bewijsvoordracht via digitale technologie gedurende het verloop van het proces, zelfs wanneer de beklaagde niet fysiek aanwezig is op de hoorzittingen.

25. De veiligheid, integriteit en betrouwbaarheid van digitale communicatie die door de autoriteiten gebruikt wordt, moet van de hoogste kwaliteit zijn.

26. Staten moeten adequate faciliteiten voorzien om rechtstreekse digitale communicatie tussen cliënten en advocaten mogelijk te maken. In het bijzonder wanneer de cliënt vastgehouden wordt.

27. De vertrouwelijkheid van digitale communicatie gebruikt in het internationale strafrecht moet onschendbaar zijn.