联合国 A/AC.291/16

大会

Distr.: General
7 November 2022
Chinese
Original: English

拟订一项关于打击为犯罪目的
使用信息和通信技术行为的
全面国际公约特设委员会
第四届会议
2023 年 1 月 9 日至 20 日，维也纳

关于打击为犯罪目的使用信息和通信技术全面国际公约的总则、刑事定罪条款及程序措施和执法条款的合并谈判文件

主席的说明

1. 为筹备拟订打击为犯罪目的使用信息和通信技术全面国际公约特设委员会第四届会议，并根据特设委员会第一届会议核准的路线图和工作方式，委员会主席在秘书处的支持下，编写了一份根据公约草案总则和刑事定罪条款及程序措施和执法条款的一读结果拟订的合并谈判文件（见附件）。

2. 更具体地说，合并谈判文件借鉴了 A/AC.291/9、A/AC.291/9/Add.1、A/AC.291/9/Add.2 和 A/AC.291/9/Add.3 号文件所汇编的会员国提案的要点，以及会员国在第二届会议期间所作的发言和发表的意见。努力为每一项条款提出一个备选案文，其中纳入了取自不同提案或发言的内容。对某些用语使用了方括号，是为了反映一些会员国在特设委员会届会上对这些用语的使用所表示的不同意见。

3. 将根据序言部分、关于国际合作、技术援助、预防措施和执行机制的条款的一读结果以及特设委员会第三届会议对公约最后条款的一读结果编写第二份合并谈判文件，并将在委员会第五届会议之前将该文件提交委员会审议。

附件

关于打击为犯罪目的使用信息和通信技术全面国际公约的总则、刑事定罪条款及程序措施和执法条款的合并谈判文件

第一章
总则

第 1 条. 宗旨声明

本公约的宗旨是：

(a) 促进和加强措施，预防和打击[为犯罪目的使用信息和通信技术][网络犯罪]，同时保护信息和通信技术用户免遭此类犯罪之害；

(b) 促进、便利和加强在预防和打击[为犯罪目的使用信息和通信技术][网络犯罪]方面的国际合作；以及

(c) 提供切实可行的措施，加强缔约国之间的技术援助，对国家机关进行预防和打击[为犯罪目的使用信息和通信技术][网络犯罪]进行能力建设，特别是为了发展中国家的利益，并加强和促进信息、专门知识、经验和良好做法的交流。

第 2 条. 术语的使用

[根据许多会员国在特设委员会第二届会议上所作的发言，这一条款应在界定公约的主要实质性条文之后再处理。]

第 3 条. 适用范围

1. 本公约应依其条款适用于对[为犯罪目的使用信息和通信技术][网络犯罪]的预防、侦查、调查和起诉，包括根据本公约所确立犯罪的所得的冻结、扣押、没收和返还。

2. 本公约还应适用于[本公约所列犯罪][任何刑事犯罪][严重犯罪]的电子形式证据的收集、获取、保全和共享。

3. 为施行本公约，除非另有规定，本公约所列犯罪不一定要对个人（包括法人）、财产和国家造成损害或伤害。

第 4 条. 保护主权

1. 缔约国在履行其根据本公约所承担的义务时，应当恪守各国主权平等和领土完整原则以及不干涉他国内政原则。

2. 本公约的任何规定概不赋予一缔约国在另一国领域内行使管辖权和履行该另一国本国法律规定的专属于该国机关的职能的权利。

第 5 条. 尊重人权

1. 缔约国应确保在履行其根据本公约承担的义务时遵守适用的国际人权法。

2. 缔约国应努力将性别视角纳入主流，并在为预防和打击[为犯罪目的使用信息和通信技术][网络犯罪]而采取的措施中考虑到弱势群体特别是妇女、儿童和老年人的特殊情况和需要。

第二章
刑事定罪

群组 1[1]

第 6 条. 非法访问

1. 各缔约国应采取必要的立法措施和其他措施，将故意违法访问[计算机系统][信息和通信技术系统]的全部或任何部分确立为刑事犯罪。

2. 缔约国可以规定，此犯罪须是通过违犯安全措施实施的，意图获取[计算机数据][电子/数字信息]或有其他犯罪意图，或者是针对与另一[计算机系统][信息和通信技术系统/装置]相连的[计算机系统][信息和通信技术系统/装置]实施的。

3. 此种访问有以下情节的，各缔约国均可加重处罚：

(a) 对使用者和受益者造成损害；

(b) 导致获取政府机密信息；

(c) 涉及或影响关键基础设施。

第 7 条. 非法拦截

1. 各缔约国均应采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：以技术手段违法拦截向[计算机系统][信息和通信技术系统/装置]、从[计算机系统][信息和通信技术系统/装置]或者在[计算机系统][信息和通信技术系统/装置]内非公开传输的[计算机数据][电子/数字信息]，包括载有这种[计算机数据][电子/数字信息]的[计算机系统][信息和通信技术系统/装置]的电磁发射。

2. 缔约国可以规定，此犯罪须是带有犯罪意图实施的，或者是针对与另一[计算机系统][信息和通信技术系统/装置]相连的[计算机系统][信息和通信技术系统/装置]实施的。

[1] 按群组安排只是为了构建正式会议期间举行的讨论。

第 8 条. 干扰[计算机数据][电子/数字信息]

1. 各缔约国均应采取必要的立法措施和其他措施，将故意违法输入、下载、复制、破坏、扰乱、删除、劣化、更改或抑制[计算机数据][电子/数字信息]的行为确立为刑事犯罪。

2. 缔约国可以规定第 1 款所述行为须造成严重损害。

3. 各缔约国均可在第 1 款所述行为涉及或影响关键基础设施的情况下加重处罚。

第 9 条. 干扰[计算机系统][信息和通信技术系统/装置]

1. 各缔约国均应采取必要的立法措施和其他措施，将通过输入、传输、破坏、删除、损坏、更改、扰乱或隐瞒[计算机数据][电子/数字信息]而故意违法严重妨碍[计算机系统][信息和通信技术系统/装置]运行的行为确立为刑事犯罪。

2. 各缔约国均可在第 1 款所述行为涉及或影响关键基础设施的情况下加重处罚。

第 10 条. 滥用装置和程序

1. 各缔约国均应采取必要的立法措施和其他措施，将故意违法实施的以下行为确立为刑事犯罪：

(a) 制作、销售、获取供使用、进口、分销或以其他方式提供：

㈠ 主要为实施根据本公约确立的任何犯罪而设计或改装的装置，包括程序；或者

㈡ 可用以访问[计算机系统][信息和通信技术系统/装置]的全部或任何部分的密码、访问凭证或类似的[数据][信息]；

意图将这类装置、密码、访问凭证或类似[数据][信息]用于实施[本公约关于非法访问的第 6 条、关于非法拦截的第 7 条、关于干扰[计算机数据][电子/数字信息]的第 8 条和关于干扰[计算机系统][信息和通信技术系统/装置]的第 9 条][根据本公约]确立的任何犯罪；以及

(b) 拥有本条第 1 款(a)项第㈠或第㈡目所述物项，意图用于实施[本公约关于非法访问的第 6 条、关于非法拦截的第 7 条、关于干扰[计算机数据][电子/数字信息]的第 8 条和关于干扰[计算机系统][信息和通信技术系统/装置]的第 9 条][根据本公约]确立的任何犯罪。缔约国可用法律规定拥有若干此类物项的负有刑事责任。

2. 如果本条第 1 款所述的制作、销售、获取供使用、进口、分销或以其他方式提供或拥有并非以实施根据本公约[前文几条]确立的犯罪为目的，而是例如为了在获得授权的情况下测试或保护[计算机系统][信息和通信技术系统/装置]，则不应将本条解释为对此规定了刑事责任。

3. 各缔约国均可保留不适用本条第1款的权利，但这一保留不得涉及本条第1款(a)项第㈡目所述物项的销售、分销或以其他方式提供。

群组 2

第 11 条. [与计算机有关的][与信息和通信技术有关的]伪造

1. 各缔约国均应采取必要的立法措施和其他措施，将故意违法实施的以下行为确立为刑事犯罪：以可能造成损害的方式输入、更改、删除或隐瞒[计算机数据][电子/数字信息]，造成不真实的[数据][信息]，意图使其像真实的一样在合法用途中被考虑或作为行动依据，而不论该[数据][信息]是否可直接阅读和理解。

2. 为本条的目的，缔约国可以规定存在诈骗意图或类似犯罪意图的负有刑事责任。

第 12 条. [与计算机有关的][与信息和通信技术有关的]诈骗

1. 各缔约国均应采取必要的立法措施和其他措施，将使用以下手段全部或部分在网上故意违法实施的造成他人或实体财产损失的诈骗行为确立为刑事犯罪：

(a) 以任何方式输入、更改、删除、屏蔽或隐瞒计算机数据；

(b) 以任何方式干扰[计算机系统][信息和通信技术系统/装置]的运行；

(c) 以任何方式使用[计算机系统][信息和通信技术系统/装置]欺骗或诱使他人或实体作出或不作出该人或实体本不会作出或不作出的任何行为，

有诈骗或犯罪意图，即为自己或他人违法获取：

㈠ 经济利益；或者

㈡ 犯罪人本无法获得的包括个人[数据][信息]在内的[计算机数据][电子/数字信息]。

2. 诈骗行为包括但不限于通过互联网或其他[借助网络的][数字]手段以下列方法在国内或跨境实施的活动：

(a) 通过虚假陈述进行诈骗；

(b) 通过不披露信息进行诈骗；

(c) 通过滥用职位进行诈骗，有诈骗或犯罪意图，即给他人造成损失或给他人带来金钱或其他财产受益。

第 13 条. [与计算机有关的][与信息和通信技术有关的]盗窃

1. 各缔约国均应采取必要的立法措施和其他措施，将以下行为确立为刑事犯罪：通过销毁、屏蔽、修改或复制[计算机数据][电子/数字信息]或以其他方式干扰[计算机][信息和通信技术]运行而盗窃财产或非法获取财产权利。

2. 各缔约国均可将[与计算机有关的][与信息和通信技术有关的]盗窃财产或非法获取财产权视为缔约国本国法律所界定的盗窃罪的加重处罚情节。

第 14 条. 非法使用电子支付工具

各缔约国均应采取必要的立法措施和其他措施，将以下行为确立为刑事犯罪：

(a) 伪造、制作或安装任何有助于以任何方式伪造或仿造任何电子支付工具的装置或材料。

(b) 挪用、使用或向他人提供任何支付工具的[数据][信息]，或为他人获取此类[数据][信息]提供便利；

(c) 利用[信息网络或信息技术][计算机系统]未经授权访问与任何支付工具有关的[数据][信息]；

(d) 明知是伪造的支付工具而接受该工具。

群组 3

第 15 条. 侵犯个人信息

各缔约国均应采取必要的立法措施和其他措施，将故意违法实施的以下行为确立为刑事犯罪：访问、出售、提供或者以其他方式提供途径获得含有某人个人信息的任何材料，包括与某人银行账户有关的信息，意图获取经济利益，并且随后未经有关个人同意而向任何其他人披露此类材料。

第 16 条. 与身份有关的犯罪

各缔约国均应采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：

(a) 在没有相关权利的情况下获取、接收或分发用以访问[计算机系统][计算机数据]的密码或凭证；以及

(b) 诈骗性或不诚实地使用任何其他人的电子签名、密码或任何其他唯一识别特征。

群组 4

第 17 条. 侵犯著作权

1. 各缔约国均应根据其依相关和适用的公约承担的义务，采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：利用[计算机系统][信息和通信技术系统/装置]实施本缔约国立法所界定的侵犯著作权行为，包括违法使用受著作权保护的计算机程序和数据库，以及剽窃行为，但故意和以商业规模侵犯这些公约所赋予的任何著作人身权的情况除外。

2. 各缔约国均应根据其依相关和适用的公约承担的义务，采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：利用[计算机系统][信息和通信技术系统/装置]实施本缔约国立法所界定的侵犯著作权相关权利行为，但故意、以商业规模和利用[计算机系统][信息和通信技术系统/装置]侵犯这些公约所赋予的任何著作人身权的情况除外。

3. 缔约国可以保留权利在有限的情况下不根据第 1 款和第 2 款施加刑事责任，但须有其他有效的补救措施可用，而且此种保留不减损缔约国的国际义务。

群组 5

第 18 条. 与网上儿童性虐待或性剥削材料有关的犯罪

1. 各缔约国均应采取必要的立法措施和其他措施，将故意违法实施的以下行为确立为刑事犯罪：

(a) 制作或者复制儿童性虐待或性剥削材料，目的是通过[计算机系统][信息和通信技术系统/装置]分发；

(b) 通过[计算机系统][信息和通信技术系统/装置]资助儿童性虐待或性剥削材料或者以其他方式为之提供便利；

(c) 通过[计算机系统][信息和通信技术系统/装置]控制、推销、提供、宣传、公开展示或者提供途径获得儿童性虐待或性剥削材料；

(d) 通过[计算机系统][信息和通信技术系统/装置]分发或者传送儿童性虐待或性剥削材料；

(e) 通过[计算机系统][信息和通信技术系统/装置]获取儿童性虐待或性剥削材料；

(f) 在明知的情况下获取权限访问或者拥有[计算机系统][信息和通信技术系统/装置]或[计算机数据存储介质][电子数字数据存储装置]中的儿童性虐待或性剥削材料，或者通过直播方式观看儿童从事露骨性行为；

(g) 通过[计算机系统][信息和通信技术系统/装置]参与本人明知或有理由认为与任何儿童性虐待或性剥削材料有关的任何业务或者从中获利。

2. 就第1款而言，“儿童性虐待或性剥削材料”一词应包括视觉材料，包括摄影、视频和实时流媒体，以及图画、书面材料和录音，这些材料描述：

(a) 儿童从事真实或模拟的露骨性行为；

(b) 貌似儿童的人从事真实或模拟的露骨性行为；

(c) 显示儿童从事真实或模拟的露骨性行为的真实图像；

(d) 主要为性目的而对儿童的性器官进行的任何描述；

(e) 遭受酷刑或残忍、不人道或有辱人格的待遇或处罚的被害人。

3. 就第 2 款而言，“儿童”一词应包括未满 18 岁的所有人。

4. 缔约国应适当考虑避免对自制第 2 款所述材料的儿童进行刑事定罪，并考虑到有必要遵守其根据《儿童权利公约》及其各项议定书承担的义务。

5. 各缔约国均可保留权利不适用第 1 款(e)和(f)项以及第 2 款(b)和(c)项的全部或部分规定。

第 19 条. 通过[计算机系统][信息和通信技术系统/装置]为儿童性虐待或性剥削材料提供便利

1. 各缔约国均应采取必要的立法措施和其他措施，依据本国法律将故意无合法理由实施的以下行为确立为刑事犯罪：创建、开发、变更、维护、控制、调节、协助、提供、宣传或推销[计算机系统][信息和通信技术系统/装置]，以便为本公约第 18 条所述儿童性虐待或性剥削材料提供便利。

2. 就第 1 款而言，“为儿童性虐待或性剥削材料提供便利”一语应包括第 1 款所述的为了使人得以获取或制作儿童性虐待或性剥削材料或者使人得以向本人或其他人传送、分发、提供或提供途径获得此类材料而实施的任何行为。

第 20 条. 通过[计算机系统][信息和通信技术系统/装置]为性目的而诱骗或诱拐儿童

1. 各缔约国均应采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：通过[计算机系统][信息和通信技术系统/装置]诱骗、允许、诱拐、教唆、胁迫或[引诱][怂恿]儿童、与儿童作出安排或向儿童提议，以便利、鼓励、提供或唆使儿童或据信是儿童的人进行或者与儿童或据信是儿童的人进行违法性行为，或者使儿童目睹或以其他方式从事性活动。

2. 就第 1 款而言，应适用[关于“儿童”的定义和儿童的刑事责任的]第 2 条[(x)]。此外，“儿童”亦包括据信未满 18 岁的人。

3. 如果一个人已采取合理步骤确定对方不是儿童，则不确立刑事责任。

第 21 条. 网上跟踪儿童

各缔约国均应采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：使用[计算机系统][信息和通信技术系统/装置]汇编、传送、发布、复制、购买、出售、接收、交换或传播儿童的姓名、电话号码、电子邮箱地址、居住地址、照片、身体描述、特征或任何其他身份识别信息，以推动安排与儿童会面以进行性交、露骨性行为或违法性活动。

群组 6

第 22 条. 未成年人参与实施非法行为

各缔约国均应采取必要的立法措施和其他措施，将以下行为确立为刑事犯罪：使用[计算机系统][信息和通信技术系统/装置]使未成年人参与实施危及其生命或身心健康的非法行为，但本公约[关于鼓励或胁迫自杀的]第[23]条中规定的行为除外。

第 23 条. 鼓励或胁迫自杀

各缔约国均应采取必要的立法措施和其他措施，将以下行为确立为刑事犯罪：通过使用[计算机系统][信息和通信技术系统/装置]施加心理压力或其他形式的压力，从而鼓励或胁迫包括儿童在内的人自杀。

群组 7

第 24 条. 性勒索

1. 各缔约国均应采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：威胁以电子手段分发或传送他人的私密图像，其具体意图是：

(a) 骚扰、威胁、胁迫、恐吓该人或对该人施加任何不正当影响，特别是为了获取经济利益或其他物质利益，包括强迫被害人从事违背其意愿的性活动；或者

(b) 获取经济利益或其他物质利益，包括强迫被害人从事违背其意愿的性活动。

2. 就第1款而言，“私密图像”系指以包括照片拍摄、影片录制或视频录制在内的任何方式对一个人进行的视觉记录：

(a) 其中该人裸体，暴露其生殖器官、肛区或乳房，或进行露骨性活动；

(b) 就此而言，在录制时，存在引起对隐私产生合理期望的情况；以及

(c) 就此而言，在犯罪实施时，该人仍有合理的隐私期望。

第 25 条. 未经同意传播私密图像

1. 各缔约国均应采取必要的立法措施和其他措施，将故意违法实施的以下行为确立为刑事犯罪：利用[计算机系统][信息和通信技术系统/装置]发布、分发、传输、销售、提供途径获取或宣传某个人的私密图像，[意图造成严重的精神痛苦]，尽管明知该图像中描绘的人没有同意该行为，或不顾该人是否同意该行为。

2. 就第1款而言，“私密图像”系指以包括照片拍摄、影片录制或视频录制在内的任何方式对一个人进行的视觉记录：

(a) 其中该人裸体，暴露其生殖器官、肛区或乳房，或进行露骨性活动；

(b) 就此而言，在录制时，存在引起对隐私产生合理期望的情况；以及

(c) 就此而言，在犯罪实施时，该人仍有合理的隐私期望。

3. 如果未经同意的分享具有合法目的，则不确立刑事责任。

4. 儿童无能力同意张贴以其为主题的私密图像。

群组 8

第 26 条. 煽动颠覆活动或武装活动

各缔约国均应采取必要的立法措施和其他措施，在本国法律下将利用信息和通信技术发出号召进行颠覆活动或武装活动以暴力推翻他国政权确立为犯罪。

第 27 条. 与极端主义有关的犯罪

各缔约国均应采取必要的立法措施和其他措施，将以下行为确立为刑事犯罪：利用[计算机系统][信息和通信技术系统/装置]散布材料号召作出以政治、意识形态、社会、种族、族裔或宗教仇恨为动机的非法行为、为此类行为进行宣传和辩护以及提供获取此类材料的途径。

第 28 条. 对种族灭绝或危害和平与人类罪的否认、认可、辩护或平反

各缔约国均应采取必要的立法措施和其他措施，在本国法律下将以下行为确立为犯罪：[以与计算机有关的方式][以与信息和通信技术有关的方式]故意传播材料对与 1945 年 8 月 8 日《伦敦协定》设立的国际军事法庭的判决书所确定的种族灭绝罪或危害和平与人类罪相当的行为予以否认、认可、辩护或平反。

群组 9

第 29 条. 与恐怖主义有关的犯罪

各缔约国均应采取必要的立法措施和其他措施，将利用信息和通信技术实施的以下行为确立为刑事犯罪：实施恐怖主义行为，煽动、招募或以其他方式参与恐怖主义活动，鼓吹恐怖主义或为其辩护，或者为资助恐怖主义而筹集或提供资金，为恐怖主义行为提供培训，便利恐怖主义组织与其成员之间的联系，包括建立、公布或使用网站，或向恐怖主义行为的实施者提供后勤支助，

传播特别是用于恐怖主义行为的爆炸物的制造方法，以及传播冲突、煽动行为或言论、仇恨或种族主义。

第 30 条. 与分销麻醉药品和精神药物有关的犯罪

各缔约国均应采取必要的立法措施和其他措施，将利用[信息和通信技术系统/装置][计算机系统]故意非法贩运麻醉药品和精神药物以及制造麻醉药品和精神药物所需材料的行为确立为刑事犯罪。

第 31 条. 与贩运武器有关的犯罪

各缔约国均应采取必要的立法措施和其他措施，将利用信息和通信技术故意非法贩运武器、弹药、爆炸装置和爆炸物质的行为确立为刑事犯罪。

第 32 条. 非法分销假冒药品和医疗产品

各缔约国均应采取必要的立法措施和其他措施，将利用信息和通信技术故意非法分销假冒药品和医疗产品的行为确立为刑事犯罪。

群组 10

第 33 条. 洗钱

1. 各缔约国均应根据本国法律基本原则采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：

(a) ㈠明知财产系犯罪所得，为隐瞒或掩饰该财产的非法来源或者为协助任何参与实施上游犯罪者逃避其行为的法律后果而转换或者转移该财产，包括虚拟货币；

㈡ 明知财产系犯罪所得而隐瞒或掩饰该财产的真实性质、来源、位置、处置、转移、所有权或与之有关的权利；

(b) 在符合本国法律制度基本概念的情况下：

㈠ 在得到财产时，明知其系犯罪所得而仍获取、拥有或者使用；

㈡ 对本条所确立的任何犯罪的参与、协同或者共谋实施、实施未遂以及协助、教唆、便利和参谋实施；

2. 为施行或者适用本条第 1 款：

(a) 各缔约国均应寻求将本条第 1 款适用于范围最为广泛的上游犯罪；

(b) 各缔约国均应将根据本公约确立的相关犯罪列为上游犯罪。缔约国立法中如果列出具体上游犯罪清单，则至少应在这类清单中列入与[为犯罪目的使用信息和通信技术][网络犯罪]有关的范围全面的各种犯罪；

(c) 就(b)项而言，上游犯罪应包括在有关缔约国法域之内和之外实施的犯罪。但是，如果犯罪是在一缔约国法域之外实施的，则只有当该行为根据其发生地所在国的国内法为刑事犯罪，而且若发生在施行或者适用本条的缔约国时根据其国内法也构成刑事犯罪时，才构成上游犯罪；

(d) 各缔约国均应向联合国秘书长提供本国施行本条的法律副本以及这类法律随后的任何修改的副本或相关说明；

(e) 如果缔约国本国法律基本原则要求，则可以规定本条第 1 款所列犯罪不适用于实施上游犯罪的人。

第 34 条. 妨害司法

各缔约国均应采取必要的立法措施和其他措施，将故意实施的以下行为确立为刑事犯罪：

(a) 在涉及本公约所涵盖的犯罪的诉讼中使用暴力、威胁或恐吓，或许诺、提议给予或给予不正当好处，以诱使提供虚假证言或干扰证言或证据的提供；

(b) 使用暴力、威胁或恐吓，干扰司法或执法人员针对本公约所涵盖的犯罪执行公务。本项规定概不应影响缔约国制定保护其他类别公职人员的立法的权利。

群组 11

第 35 条. 法人责任

1. 各缔约国均应采取符合其法律原则的必要的立法措施和其他措施，对于在法人机构中担任领导职务的任何自然人不论是作为个人还是作为法人机构的一部分基于下述权力为法人利益实施的本公约确立的刑事犯罪，确定该法人对此犯罪的责任：

(a) 法人代表权；

(b) 代表法人作出决定的职权；

(c) 在法人内部行使控制权的职权。

2. 除本条第 1 款已规定的情况之外，各缔约国均应采取必要措施确保，如果因第 1 款所述自然人缺乏监督或控制而使某一自然人在其明示或默示职权范围内行事时有可能为法人利益实施根据本公约确立的刑事犯罪，则可对法人追究责任。

3. 在不违反缔约国法律原则的情况下，法人责任可以是刑事责任、民事责任或行政责任。

4. 此种责任不应影响实施这种犯罪的自然人的刑事责任。

5. 各缔约国均应特别确保使根据本条被追究责任的法人受到有效、适度和劝阻性的刑事或非刑事处罚，包括金钱处罚。

6. 法人应受保护，在以下情况下免于为出于善意而作出或不作出的行为承担责任：

(a) 在履行或打算履行本公约所规定的义务时；或者

(b) 在行使或打算行使本公约赋予或规定的职能或权力时。

第 36 条. 参与和未遂

1. 各缔约国均应采取必要的立法措施和其他措施，根据本国法律，将以共犯、从犯、煽动犯、教唆犯或同谋犯等任何身份参与根据本公约确立的犯罪确立为刑事犯罪。

2. 各缔约国均可以采取必要的立法措施和其他措施，根据本国法律，将故意实施根据本公约确立的犯罪的任何未遂行为确立为刑事犯罪。

3. 各缔约国均可以采取必要的立法措施和其他措施，根据本国法律，将故意为根据本公约确立的犯罪进行的预备确立为刑事犯罪。

4. 各缔约国均应采取必要的立法措施和其他措施，加强对集体犯罪，包括对有组织犯罪集团所犯罪行追究责任。

5. 各缔约国均可以保留全部或部分不适用本条第 2 款的权利。

第 37 条. 作为犯罪要件的明知、意图和目的

根据本公约确立的犯罪需具备的明知、意图或目的等要件可以根据客观实际情况予以推定。

第 38 条. 追诉时效

各缔约国均应根据本国法律酌情确定一个长的追诉时效期，以在此期限内对根据本公约确立的任何犯罪启动诉讼程序，并对被指控犯罪人已经逃避司法处置的情形确定更长的追诉时效期或者作出关于中止追诉时效的规定。

第 39 条. 起诉、审判和处罚

1. 各缔约国均应对实施根据本公约确立的犯罪进行与其严重性相当的处罚。

2. 各缔约国均可以对根据本公约确立的犯罪加重处罚，包括但不限于犯罪的以下情节：

(a) 影响关键基础设施；

(b) 导致获取政府机密信息；

(c) 对个人造成伤害，包括身体或心理创伤。

3. 各缔约国均应根据本国法律制度和宪法原则采取必要措施以建立或者保持一种适当的平衡，既顾及为公职人员履行其职能所给予的豁免或者司法特权，也顾及在必要时对根据本公约确立的犯罪进行有效的侦查、起诉和审判的可能性。

4. 各缔约国均应努力确保，为根据本公约确立的犯罪起诉某人时依据本国法律行使的任何法律裁量权对这些犯罪的执法措施取得最大成效，并适当考虑到震慑这种犯罪的必要性。

5. 各缔约国均应确保因根据本公约确立的犯罪而被起诉的任何人享有符合其所在国法律及国际人权法相关和适用条款的一切权利和保障，包括享有公正审判的权利和辩护权。

6. 就根据本公约确立的犯罪而言，各缔约国均应根据本国法律并在适当尊重辩护权的情况下采取适当措施，力求确保对于有关保外候审或上诉的裁决所规定的条件考虑到需要确保被告人在其后的刑事诉讼中出庭。

7. 各缔约国均应在考虑被判定实施了有关犯罪的人员早释或者假释的可能性时，顾及这种犯罪的严重性。

8. 本公约的任何规定概不影响以下原则，即根据本公约确立的犯罪、适用的法律辩护或其他决定行为合法性的法律原则均留给缔约国国内法予以说明，并且应根据该国内法起诉和惩罚此类犯罪。

9. 缔约国应努力促进被判定实施了根据本公约确立的犯罪的人员重新融入社会。

第三章
程序措施和执法

群组 1

第 40 条. 管辖权

1. 各缔约国均应在下列情况下采取必要的措施，对根据本公约确立的犯罪确立管辖权：

(a) 犯罪发生在该缔约国的领域内；或者

(b) 犯罪发生在当时悬挂该缔约国国旗的船只上或已根据该缔约国法律注册的航空器内。

2. 在不违背本公约第 4 条规定的情况下，缔约国还可以在下列情况下对任何此种犯罪确立其管辖权：

(a) 犯罪系针对该缔约国的国民或法人；或者

(b) 犯罪者为该缔约国的国民或法人或者在该国领域内有惯常居所的无国籍人；或者

(c) 犯罪发生在该国领域之外，但目的是在其领域内实施根据本公约确立的犯罪；或者

(d) 犯罪系针对该缔约国；或者

(e) 犯罪涉及该缔约国的国民的[计算机数据][电子/数字信息]，而不论其实际存储、处理或筛选的地点。

3. 为本公约关于引渡的条文的目的，各缔约国均应采取必要措施，在被指控犯罪人在其领域内且仅因该人系本国国民而不予引渡时，对根据本公约确立的犯罪确立本国的管辖权。

4. 各缔约国还可以采取必要的措施，在被指控犯罪人在其领域内且不引渡该人时对根据本公约确立的犯罪确立本国的管辖权。

5. 如果根据本条第 1 款或第 2 款行使管辖权的缔约国被告知或者通过其他途径获悉任何其他缔约国正在对同一行为进行侦查、起诉或者司法程序，则这些缔约国的主管机关应酌情相互磋商，以便协调行动。

6. 在不影响一般国际法准则的情况下，本公约不排除缔约国行使其根据本国法律确立的任何刑事管辖权。

第 41 条. 程序措施的范围

1. 各缔约国均应采取必要的立法措施和其他措施，确立本章所规定的权力和程序，以便进行具体的刑事侦查或诉讼。

2. 除本公约第 48 条另有规定外，各缔约国均应将本条第 1 款所述权力和程序适用于：

(a) 根据本公约确立的刑事犯罪；

(b) 利用[计算机系统][信息和通信技术系统/装置]实施的其他刑事犯罪；以及

(c) 收集[本公约所述犯罪][任何刑事犯罪][严重犯罪]的电子形式证据。

3. (a)各缔约国均可保留权利将本公约第 47 条所述措施仅适用于保留意见中具体所指的犯罪或犯罪类别，条件是这些犯罪或犯罪类别的范围不得比缔约国适用第 48 条所述措施的刑事犯罪的范围更小。各缔约国均应考虑限制此类保留，以使实时收集流量数据的措施能够得到最广泛的适用。

(b) 若缔约国因本公约通过时实行的立法所限，不能对服务提供者的[计算机系统][信息和通信技术系统/装置]内传输的信息适用实时收集流量数据和拦截内容数据的措施，而该系统：

㈠ 正在为一个封闭用户群的利益运行；以及

㈡ 不使用公共通信网络，也不与另一个公共或私人计算机系统连接；

则该缔约国可保留不对此类通信适用上述措施的权利。各缔约国均应考虑限制此类保留，以使实时收集流量数据和拦截内容数据的措施能够得到最广泛的适用。

第 42 条. 条件和保障措施

1. 各缔约国均应确保本章规定的权力和程序的确立、实施和适用符合本国国内法规定的条件和保障措施，国内法应规定充分保护人权和自由，包括因其根据适用的国际人权法承担的义务而产生的权利和基本自由，并应纳入罚当其罪原则、谦抑原则和罪刑法定原则以及对隐私和个人数据的保护。

2. 这种条件和保障措施应当鉴于有关程序或权力的性质等，酌情包括对这种权力或程序的司法监督或其他独立监督、适用这种权力或程序的正当理由以及这种权力或程序的范围和期限限制。

3. 在符合公共利益、特别是稳健司法的范围内，各缔约国均应考虑本条规定的权力和程序对第三方权利、责任和合法利益的影响。

群组 2

第 43 条. 快速保全[存储的计算机数据]
[累积的电子/数字信息]

1. 各缔约国均应采取必要的立法措施和其他措施，使其主管机关能够发出适当的命令或指示，或以类似方式获取或确保快速保全通过[计算机系统][信息和通信技术系统/装置]存储的指定[计算机数据][电子/数字信息]，包括流量数据，特别是在有理由认为该[计算机数据][电子/数字信息]极易被删除、复制、丢失或修改，包括由于其国内法或提供者的服务条款规定的保留期期满而出现这些问题的情况下。

2. 如果缔约国施行上文第 1 款，下令某人，包括法人，保全其拥有或控制的所存储的指定[计算机数据][电子/数字信息]，则该缔约国应采取必要的立法措施和其他措施，责成该人在必要的一段时间，最长不超过 90 天，保全和维护该[计算机数据][电子/数字信息]的完整性，以使主管机关能够寻求予以披露。缔约国可规定这种命令嗣后可以延期。

3. 各缔约国均应采取必要的立法措施和其他措施，责成保管人或其他负责保全[计算机数据][电子/数字信息]的人员在其国内法规定的期限内对采取此类程序事宜保密。

4. 本条所述权力和程序应根据本公约第 41 条和第 42 条予以确定。

第 44 条. 快速保全和部分披露流量数据

1. 对于根据关于快速保全存储的[计算机数据][电子/数字信息]的条文的规定应予保全的流量数据，各缔约国均应采取必要的立法措施和其他措施，以便：

(a) 确保快速保全流量数据，无论该通信的传输涉及一个还是多个服务提供者；以及

(b) 确保向该缔约国的主管机关或该机关所指定人员快速披露足够数量的流量数据，以使该缔约国能够确定服务提供者，并确定通信或所指信息的传输路径。

2. 本条所述权力和程序应以第 41 条和第 42 条为前提。

第 45 条. 提交令

1. 各缔约国均应采取必要的立法措施和其他措施，授权本国主管机关在有合理理由认为已经实施或正在实施刑事犯罪的情况下，下令：

(a) 本国领域内的某人提交其所拥有或控制的存储在计算机系统或计算机数据存储介质中的指定[计算机数据][电子/数字信息]；以及

(b) 在本缔约国领域内提供服务的服务提供者提交其所拥有或控制的与此类服务有关的用户信息。

2. 本条所述权力和程序应以第 41 条和第 42 条为前提。

3. 就本条而言，“用户信息”一词系指服务提供者掌握的以[计算机数据][电子/数字信息]形式或任何其他形式包含的任何信息，这些信息与其服务的用户而非流量数据或内容数据有关，通过这些信息有可能确定：

(a) 使用的信息和通信技术服务类型、对其适用的技术规定以及服务期；

(b) 根据服务协议或安排提供的用户身份、邮政或地理地址、电话和其他接入号码、账单和付款信息；

(c) 根据服务协议或安排提供的信息和通信设备的位置的有关信息。

第 46 条. 搜查和扣押[以电子/数字方式存储或处理的信息][存储的计算机数据]

1. 各缔约国均应采取必要的立法措施和其他措施，授权本国主管机关在有合理理由认为已经实施或正在实施刑事犯罪的情况下，在本国领域内或根据本国管辖权搜查或以类似方式访问：

(a) [信息和通信技术系统/装置][计算机系统]或其一部分以及存储在其中的[计算机数据][电子/数字信息]；以及

(b) 可以存储所查找的[计算机数据][电子/数字信息]的[计算机数据][电子/数字信息]存储介质。

2. 各缔约国均应采取必要的立法措施和其他措施，以确保若其主管机关根据本条第 1 款(a)项的规定进行搜查时有合理理由认为所查找的[计算机数据][电子/数字信息]存储在本国领域内另一[信息和通信技术系统/装置][计算机系统]中，而且这类[数据][信息]可从初始系统合法访问或可供初始系统合法取用，则该主管机关应能够快速进行搜查，以得以访问该其他[信息和通信技术系统/装置][计算机系统]或其中包含的[数据][信息]。

3. 各缔约国均应采取必要的立法措施和其他措施，授权其主管机关在本国领域内或根据本国管辖权扣押或以类似方式取得根据第 1 款或第 2 款访问的[计算机数据][电子/数字信息]，或以类似方式取得这类信息。这些措施应包括以下权力：

(a) 扣押或以其他方式取得[信息和通信技术系统/装置][计算机系统]、其一部分或用于存储[计算机数据][电子/数字信息]的介质；

(b) 以电子/数字形式制作和保留[计算机数据][电子/数字信息]的副本；

(c) 维护所存储的相关[计算机数据][电子/数字信息]的完整性；

(d) 使被访问的[计算机系统][信息和通信技术系统/装置]无法访问，或者删除其中的[计算机数据][电子/数字信息]。

4. 各缔约国均应采取必要的立法措施和其他措施，授权其主管机关下令对有关[信息和通信技术系统/装置][计算机系统]的运行、信息和电信网络或其组成部件或为保护其中的[计算机数据][电子/数字信息]而适用的措施具有专门知识的任何人提供合理的必要信息，以使得能够采取本条第 1 款至第 3 款所述措施。

5. 本条所述权力和程序应以第 41 条和第 42 条为前提。

第 47 条. 实时收集流量数据

1. 各缔约国均应采取必要的立法措施和其他措施，授权其主管机关在有合理理由认为已经实施或正在实施刑事犯罪的情况下，在本缔约国领域内对通过[计算机系统][信息和通信技术系统/装置]传送的与其境内的特定通信有关的流量数据采取下列行动：

(a) 在本缔约国领域内通过应用技术手段实时收集或记录；以及

(b) 迫使服务提供者在其现有的技术能力范围内：

㈠ 在本缔约国领域内通过应用技术手段实时收集或记录；或者

㈡ 配合并协助主管机关实时收集或记录；

与本缔约国领域内的特定信息有关的此类数据。

2. 缔约国由于其国内法律制度基本原则而不能采取第 1 款(a)项所述措施的，可代之以采取必要的立法措施和其他措施，确保在其领域内通过应用技术手段实时收集或记录与在其领域内传输的特定通信有关的流量数据。

3. 各缔约国均应采取必要的立法措施和其他措施，责成服务提供者对行使本条所规定的任何权力的事实和与之有关的任何信息保密。

4. 本条所述权力和程序应以第 41 条和第 42 条为前提。

第 48 条. 拦截内容数据

1. 各缔约国均应针对拟由国内法确定的一系列严重犯罪采取必要的立法措施和其他措施，授权其主管机关针对在本国领域内利用[计算机系统][信息和通信技术系统/装置]传输的特定通信的[内容数据][利用信息和通信技术传输的电子/数字信息，包括内容数据]采取下列行动：

(a) 在本缔约国领域内应用技术手段实时收集或记录；以及

(b) 迫使服务提供者在其现有的技术能力范围内：

㈠ 在本缔约国领域内应用技术手段实时收集或记录；或者

㈡ 配合并协助主管机关实时收集或记录；

此类[数据][信息]。

2. 缔约国由于其本国法律制度基本原则而不能采取第 1 款(a)项所述措施的，可代之以采取必要的立法措施和其他措施，确保在其领域内应用技术手段实时收集或记录关于在其领域内的特定通信的内容数据。

3. 各缔约国均应采取必要的立法措施和其他措施，责成服务提供者对行使本条所规定的任何权力的事实和与之有关的任何信息保密。

4. 本条所述权力和程序应以第 41 条和第 42 条为前提。

第 49 条. 采纳[电子/数字]证据

从装置、设备、电子/数字介质、信息系统、计算机程序或任何信息和通信技术中获得或提取的电子/数字证据，符合有关缔约国的法律所规定的技术条件的，应具有刑事诉讼程序中重大法证证据的证明价值。

群组 3

第 50 条. 冻结、扣押和没收犯罪所得

1. 各缔约国均应在国内法律制度的范围内尽最大可能采取必要措施，以使得能够没收：

(a) 来自根据本公约确立的犯罪的犯罪所得或者价值与这种所得相当的财产；

(b) 用于或者拟用于根据本公约确立的犯罪的财产、设备或者其他工具。

2. 各缔约国均应采取必要措施，使得能够辨认、追查、冻结或扣押本条第 1 款所述任何物品，以便最终予以没收。

3. 各缔约国均应根据本国法律采取必要的立法措施和其他措施，规范主管机关对本条第 1 款和第 2 款涵盖的所冻结、扣押或没收财产的管理。

4. 如果犯罪所得已经部分或者全部转变或者转化为其他财产，则应以此类财产代替犯罪所得，适用本条所述措施。

5. 如果犯罪所得已经与从合法来源获得的财产相混合，则应当在不影响冻结权或扣押权的情况下没收这类财产，没收价值最高可以达到混合于其中的犯罪所得的估计价值。

6. 对于来自犯罪所得、来自犯罪所得转变或者转化而成的财产或者来自已经与犯罪所得相混合的财产的收入或者其他利益，也应当适用本条所述措施，处置方式和程度与处置犯罪所得相同。

7. 为本公约的本条和[关于没收事宜国际合作的]条文的目的，各缔约国均应授权其法院或其他主管机关下令提供或扣押银行记录、财务记录或商业记录。缔约国不得以银行保密为由拒绝按照本款规定采取行动。

8. 各缔约国均可考虑能否要求由犯罪人证明应予没收的涉嫌犯罪所得或其他财产的合法来源，但此种要求应符合其国内法原则以及司法程序和其他程序的性质。

9. 不得对本条的规定作损害善意第三方权利的解释。

10. 本条的任何规定概不影响以下原则，即本条所述措施应根据缔约国国内法的规定予以界定和实施。

第 51 条. 建立犯罪记录

各缔约国均可采取必要的立法措施或其他措施，按其认为适宜的条件并为其认为适宜的目的，考虑别国以前对被指控犯罪人作出的任何有罪判决，以便在涉及根据本公约确立的犯罪的刑事诉讼中利用这类信息。

第 52 条. 保护证人

1. 各缔约国均应在其力所能及的范围内采取适当措施，有效保护对根据本公约确立的犯罪提供证言或者善意地并基于合理理由提供信息或者以其他方式与侦查机关或司法机关配合的证人，并酌情为其亲属和其他与其关系密切的人提供有效保护，使其免遭可能的报复或恐吓。

2. 在无损于被告人的权利包括正当程序权的情况下，本条第1款所述措施可包括：

(a) 制定向此类人员提供人身保护的程序，例如，在必要和可行的情况下将其转移，并在适当情况下允许不披露或者限制披露有关其身份和下落的信息；

(b) 规定证据规则，允许证人以确保其安全的方式作证，例如允许借助于视频链接之类的通信技术或其他适当手段提供证言。

3. 缔约国应考虑与其他国家订立有关转移本条第 1 款所述人员的协议或安排。

4. 本条的规定也应适用于作为证人的被害人。

第 53 条. 帮助和保护被害人

1. 各缔约国均应在其力所能及的范围内采取适当的措施，向根据本公约确立的犯罪的被害人提供帮助和保护，尤其是在有报复威胁或恐吓的情况下。

2. 各缔约国均应制定适当的程序，使根据本公约确立的犯罪的被害人有机会获得赔偿和补偿。

3. 各缔约国均应在符合国内法的情况下，在对犯罪人提起的刑事诉讼的适当阶段，以不损害辩护方权利的方式使被害人的意见和关切得到表达和考虑。

第 54 条. 损害赔偿

各缔约国均应根据国内法原则采取必要的措施，确保因[为犯罪目的使用信息和通信技术][网络犯罪]而受到损害的实体或者人员有权为获得赔偿而对这种损害的责任者提起诉讼程序。

第 55 条. 加强与执法机关配合的措施

1. 各缔约国均应采取适当措施，鼓励参与或曾参与根据本公约确立的犯罪的人员：

(a) 就如下事项为主管机关的侦查和取证提供有用信息：

㈠ 参与根据本公约确立的犯罪的人员的身份、性质、组成情况、结构、所在地或活动；

㈡ 与参与根据本公约确立的犯罪的其他人员的联系，包括国际联系；

㈢ 参与根据本公约确立的犯罪的人员已经实施或可能实施的其他犯罪；

(b) 向主管机关提供可能有助于剥夺参与根据本公约确立的犯罪的人员的资源或犯罪所得的实际、具体的帮助。

2. 对于在根据本公约确立的犯罪的侦查或者起诉中提供实质性配合的被告人员，各缔约国均应考虑就适当情况下减轻处罚的可能性作出规定。

3. 对于在根据本公约确立的犯罪的侦查或者起诉中提供实质性配合的人员，各缔约国均应考虑根据国内法基本原则就允许免予起诉的可能性作出规定。

4. 应按本公约关于保护证人的条文的规定为此类人员提供保护。

5. 如果本条第 1 款所述的、处于某一缔约国的人员能够给予另一缔约国主管机关以实质性配合，则有关缔约国可以考虑根据国内法订立关于可能由对方缔约国提供本条第 2 款和第 3 款所述待遇的协议或者安排。