联合国 A/AC.291/9/Add.2

大 会

Distr.: General
21 April 2022
Chinese
Original: Arabic/English/Spanish/
Russian

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
第二届会议
2022 年 5 月 30 日至 6 月 10 日，维也纳

会员国就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的刑事定罪条款、总则及关于程序措施和执法的条款提交的提案和材料汇编

增编

V.22-02334 (C) 310522 030622

目录

四. 程序措施和执法

安哥拉

[原文：英文]
[2022 年 4 月 8 日]

程序规定和执法

证据手段：书面证据（电子文件、数字文件）、专家证据（计算机专门知识）。

取证手段：网上搜索、快速保全数据、快速披露数据、强制提交或准予访问数据、搜查计算机数据、扣押计算机数据、扣押电子邮件和记录类似性质的通信、拦截通信、隐藏行动（深网和暗网）。

为国家追回资产和资产损失：扣押和没收传统资产和加密资产。

本章的规定应适用于调查和刑事起诉传统犯罪的犯罪分子，而不仅仅是调查网络犯罪。

为了阐明与本章有关的概念，可以以上文提到的区域和国际法律文书为依据。[1]

澳大利亚

[原文：英文]
[2022 年 4 月 13 日]

刑事定罪和程序性权力之间的联系

澳大利亚认识到，各国不妨确保该公约为请求和获取位于另一个法域内与实施涉及或不涉及网络层面的常见犯罪（如非法侵入或谋杀）有关的电子证据提供框架，改善审办这类犯罪的国际合作。

该公约的侦查、调查和起诉网络犯罪的程序性权力、调查权力和国际合作框架应适用于公约中所列犯罪，但不应仅限于适用于这些犯罪。

该公约规定的程序性权力（详见下文）应适用于借助计算机系统或数字技术实施的其他刑事犯罪，也适用于收集侦查、调查和起诉实施时不涉及计算机系统的刑事犯罪所需的电子证据，但这种收集须达到这些程序性权力的规定条件和门槛。

同样，该公约规定的国际合作框架不仅应适用于公约创设的刑事犯罪，而且，在适当的情况下，也适用于借助计算机实施的其他刑事犯罪，以及适用于收集侦查、调查和起诉动态刑事犯罪所需的电子证据。

因此，“刑事定罪”一章的目的不是限制公约其他章节运作，而是为一种相对较新的犯罪类型——网络犯罪——在所有国家确立一个共同标准。

[1] 秘书处的说明：本脚注提及纳入不同小标题下的文书：《非洲联盟网络安全和个人数据保护公约》、《欧洲委员会网络犯罪公约》、《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》。

打击网络犯罪的程序措施

程序法是调查和起诉网络犯罪的关键要素。该公约应提供明确的程序措施框架，以确保执法机关能够获得打击网络犯罪所需的证据，以维护法治的强有力程序保障和限制及对人权和基本自由的保护为基础。公约中关于程序措施的条款也应尊重现有的框架，并避免现有国际文书不成体系。

程序措施应适用于该公约规定的实质性刑事犯罪，并且按照各缔约国的本国法律框架，适用于借助计算机系统或数字技术实施的其他刑事犯罪，以及适用于收集侦查、调查和起诉动态刑事犯罪所需的电子证据，这种收集须达到这些程序性权力的规定条件和门槛。

澳大利亚建议在新公约中列入以下程序措施：

- 保全电子数据（包括存储的内容数据、用户信息和流量数据）的命令
- 提交电子数据的命令
- 搜查和扣押电子数据
- 实时收集电子数据（包括流量数据和实时拦截内容数据）
- 紧急和加快保全和提交数据的命令。

程序措施应顾及电子数据的性质，以确保快速有效地保全数据；执法和其他相关机关可以快速有效地获得这类数据，以确保网络空间中的犯罪方法和做法不会干扰各机关的收集工作。

程序措施的条件、要求和保障措施

侦查、调查和起诉网络犯罪的程序措施可能涉及相关国际人权文书，包括《公民及政治权利国际公约》规定的人权和自由方面的义务。这些权利和义务可能包括：

公正审判和公正审理权（《公民及政治权利国际公约》，第十四条）

《公约》第十四条载有公正审判和公正审理权，包括程序保障、法治和无罪推定。人权事务委员会指出：“《公约》第十四条旨在确保正当的司法，并为此目的保障一系列具体权利”。

第十四条不是一项绝对的权利，须受到容许的限制，条件是这些限制是依法规定的，并且是追求合法目标合理、必要和相称的手段。

隐私不受侵扰的自由（《公民及政治权利国际公约》，第十七条）

《公约》第十七条规定了隐私不受侵扰的权利，并规定“任何人的私生活、家庭、住宅或通信，不得加以任意或非法干涉”。

人权事务委员会第 16 号一般性意见更详细地阐述了这项权利的内容。此项意见指出，这种保护“必须保证不受任何这类干涉和攻击，不管是来自国家当局，还

是来自自然人或法人”。第 16 号一般性意见第 3 段指出：“‘非法’一词的意思是，除法律设想的情况外，不能进行任何干预。国家授权的干涉必须依据法律，但法律本身必须符合《公约》的规定、目的和目标。”

表达自由权（《公民及政治权利国际公约》，第十九条第 2 款）

《公约》第十九条规定了表达自由权。《公约》第十九条第 2 款承认通过任何媒介，包括书面和口头通信、媒体、广播和商业广告，寻求、接收和传播各种信息和思想的权利。

表达自由权不是一项绝对的权利。根据第十九条第 3 款，表达自由可依据法律规定和在必要时受到限制，以便保护他人的权利或名誉、国家安全、公共秩序或公共卫生或道德。限制必须依据立法来规定，是实现预期目的所必需的，并且与作出限制所根据的需要相称。

《公约》的目标及其程序措施旨在减少网络犯罪的威胁、影响和损害——这可能为在合法、合理、必要和相称时限制人权和自由提供一个容许的基础。

迫切需要遵照《公约》和其他适用的人权文书规定的条件和保障措施，制定、执行和适用《公约》中阐述的程序措施。

对每项程序措施而言，这类条件和保障措施应酌情包括：

- 司法或其他独立监督或监控
- 证明适用程序措施的理由
- 对程序措施的范围和持续时间的限制
- 考虑程序措施对第三方权利、责任和合法利益的影响。

巴西

[原文：英文]
[2022 年 4 月 8 日]

第三章
程序措施和执法

第 18 条
程序规定的范围[2]

1. 各缔约国均应采取必要的立法和其他措施，确立本章所设想的权力和程序，以便预防、侦查、阻止、调查、起诉和判决网络犯罪。

2. 除非另有规定，各缔约国应将本条第 1 款所述权力和程序应用于：

(a) 根据本公约第二章确定的刑事犯罪；

[2] 资料来源：中国和俄罗斯联邦的提案，巴西作了修改。

(b) 借助信息和通信技术实施的其他刑事犯罪；

(c) 收集与实施刑事犯罪有关的电子形式的证据。

第 19 条
条件和保障措施[3]

1. 各缔约国应确保本节所规定权力和程序的确立、实施和适用符合根据其本国法律规定的条件和保障措施，其中应规定充分保护人权和自由，包括根据其依《公民及政治权利国际公约》及其他适用的国际人权文书所承担的义务而产生的权利，并应纳入相称原则。

2. 鉴于有关程序或权力的性质等，此类条件和保障措施除其他外还应酌情纳入司法或其他独立监督、适用的正当理由以及此类权力或程序的范围和期限限制。

3. 在符合公共利益，特别是健全司法的范围内，各缔约国应考虑本节规定的权力和程序对第三方的权利、责任和合法利益的影响。

第 20 条
加快保全已存储的计算机数据[4]

1. 各缔约国均应采取必要的立法和其他措施，使其主管机关能够下令或以类似方式实现快速保全通过计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或修改的情况下。

2. 如果缔约国执行上文第 1 款，命令某人保全其拥有或控制的指定已存储计算机数据，该缔约国应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护该计算机数据的完整性，最长不超过 90 天，以便主管机关能够寻求披露这些数据。缔约国可规定此种命令嗣后可以延期。

3. 各缔约国应采取必要的立法和其他措施，责成保管人或其他负责保全计算机数据的人在其国内法规定的期限内对采取这类程序事宜保密。

4. 本条所述权力和程序应受第 18 条和第 19 条的约束。

第 21 条
加快保全积累的电子信息[5]

1. 各缔约国均应采取必要的立法和其他措施，使其主管机关能够下达适当的命令或指示，或以类似方式确保快速保全指定的电子信息，包括流量数据，特别是在有理由认为数据特别容易被删除、复制或修改的情况下，包括由于其国内立法或提供者服务条款规定的留存期限到期而被删除、复制或修改。

[3] 资料来源：《布达佩斯公约》以及中国和俄罗斯联邦的提案。

[4] 资料来源：《布达佩斯公约》。

[5] 资料来源：中国和俄罗斯联邦的提案。

2. 如果缔约国执行本条第 1 款的规定，命令个人（包括法人）保全其所拥有或控制的指定存储信息，该缔约国应采取必要的立法和其他法律措施，责成该人在必要长的期限内保全这类信息并维护其完整性，但不超过该缔约国本国立法确定的期限，以便主管机关能够寻求披露数据。缔约国可以规定此种命令嗣后可以延期。

3. 各缔约国均应采取必要的立法和其他措施，责成负责保全信息的人在其国内立法规定的期限内对采取这类程序事宜保密。

4. 本条所述权力和程序应按照本公约第 18 条和第 19 条的规定来确定。

第 22 条
加快保全和部分披露流量数据[6]

各缔约国应就拟保全的流量数据采取必要的立法和其他措施，以便：

(a) 确保快速保全流量数据，无论该通信传输涉及一个还是多个服务提供者；

(b) 确保向该缔约国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，以便该缔约国能够确定服务提供者和通信传输路径。

本条所述权力和程序应受第 18 条和第 19 条的约束。

第 23 条
提交令[7]

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关命令：

(a) 其境内的个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；

(b) 在缔约国境内提供服务的服务提供者提交其所拥有或控制的与这类服务有关的用户数据。

2. 本条所述权力和程序应受第 18 条和第 19 条的约束。

第 24 条
搜查和扣押以电子方式存储或处理的信息[8]

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关在该缔约国境内或根据其管辖权寻求访问：

(a) 信息和通信技术设备及其中存储的信息；

(b) 可以存储所寻求电子信息的信息存储介质。

[6] 资料来源：《布达佩斯公约》以及中国和俄罗斯联邦的提案。

[7] 资料来源：《布达佩斯公约》以及中国和俄罗斯联邦的提案，巴西作了修改。

[8] 资料来源：中国和俄罗斯联邦的提案。类似于《布达佩斯公约》第 19 条的规定，中国和俄罗斯联邦作了修改。

2. 各缔约国均应采取必要的立法和其他措施，确保若其主管机关根据本条第 1 款(a)项的规定进行搜查，有理由认为所寻求信息存储在该缔约国境内另一信息和通信技术设备中，这些主管机关应当能够快速开展搜查，以便能够访问该另一信息和通信技术设备或其中所载的数据。

3. 各缔约国均应采取必要的立法和其他措施，授权其主管机关在其境内或根据其管辖权扣押电子信息，或以类似方式取得这类信息。这些措施应包括规定以下权力：

(a) 扣押用于存储信息的信息和通信技术设备或以其他方式取得该设备；

(b) 以电子和数字形式制作并留存这类信息的副本；

(c) 维护相关所存储信息的完整性；

(d) 删除以电子方式存储或处理的信息。

4. 各缔约国均应采取必要的立法和其他措施，授权其主管机关根据其本国立法确立的程序，命令任何对有关信息系统运行、信息和电信网络或其组成部件或为保护其中的信息而适用的措施有专门知识的人，为采取本条第 1 款至第 3 款所述措施，提供必要的信息和（或）援助。

5. 本条所述权力和程序应按照本公约第 18 条和第 19 条的规定来确定。

第 25 条
实时收集流量数据[9]

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国境内用技术手段实时收集或记录，

(b) 迫使服务提供者在其现有的技术能力范围内：

㈠ 在该缔约国境内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，

与其境内以计算机系统传输的指定通信相关的流量数据。

2. 如果缔约国由于其本国法律制度的既定原则不能采取第 1 款(a)项所述措施，该缔约国可采取必要的立法和其他措施，确保在其境内用技术手段，实时收集或记录与其境内传输的指定通信有关的流量数据。

3. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条规定的任何权力以及与此有关的任何信息保密。

4. 本条所述权力和程序应受第 18 条和第 19 条的约束。

[9] 资料来源：《布达佩斯公约》。

第 26 条
拦截内容数据[10]

1. 各缔约国应针对将由本国法律确定的一系列严重犯罪，采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国境内用技术手段实时收集或记录；和

(b) 迫使服务提供商在其现有的技术能力范围内：

㈠ 在该缔约国境内用技术手段实时收集或记录；或

㈡ 配合并协助主管机关实时收集或记录，

在其境内以计算机系统传输的指定通信的内容数据。

2. 如果缔约国由于其本国法律制度的既定原则不能采取第 1 款(a)项所述措施，该缔约国可采取必要的立法和其他措施，确保在其境内用技术手段实时收集或记录其境内指定通信的内容数据。

3. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条所规定的任何权力以及与此有关的任何信息保密。

4. 本条所述权力和程序应受第 18 条和第 19 条的约束。

第 27 条
管辖权[11]

1. 各缔约国均应采取必要的立法和其他措施，在下列情况下，对依本公约第 2 条至第 11 条确定的任何犯罪确立管辖权：

(a) 犯罪发生在该缔约国境内，或者

(b) 犯罪发生在悬挂该缔约国国旗的船只上；或者

(c) 犯罪发生在根据该缔约国的法律注册的航空器内；或者

犯罪系由其国民所实施，条件是该犯罪行为根据犯罪发生地的刑法应受到惩罚，或者实施犯罪是在任何缔约国领土管辖范围之外。

2. 各缔约国可保留不适用或仅在特定情况或条件下适用本条第 1 款(b)至(d)项或其任何部分规定的管辖权规则的权利。

3. 各缔约国均应采取必要措施，对被控犯罪人在本国境内、在收到引渡请求后只以其国籍为依据不将其引渡到另一缔约国的案件确立管辖权。

4. 本公约不排除缔约国根据其本国法律行使的任何刑事管辖权。

[10] 资料来源：《布达佩斯公约》。

[11] 资料来源：《布达佩斯公约》，巴西作了修改。

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通过其他途径获悉，任何其他缔约国正对同一行为进行调查、起诉或进行司法程序，这些缔约国的主管机关应酌情相互磋商，以便协调行动。[12]

加拿大

[原文：英文]
[2022 年 4 月 9 日]

程序性权力

程序性权力的范围

1. 阐明本节规定的权力和程序，是为了进行具体的刑事侦查或诉讼。

2. 除非另有明确规定，缔约国应将第 1 款所述权力和程序应用于：

(a) 根据本公约确定的刑事犯罪；

(b) 借助计算机系统实施的其他刑事犯罪；

(c) 收集刑事犯罪的电子形式的证据。

加快保全已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施，使其国内主管机关能够下令或以类似方式实现快速保全借助计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或修改的情况下。

2. 如果缔约国执行第 1 款，命令某人保全其所拥有或控制的指定已存储计算机数据，则该缔约国应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护该数据的完整性，最长不超过 90 天，以便主管机关能够寻求披露这些数据。缔约国可规定这类命令嗣后可以延期。

3. 各缔约国均应采取必要的立法和其他措施，在有正当理由且获得授权的情况下，责成保管人或其他负责保全计算机数据的人在其本国法律规定的期限内对采取这类程序事宜保密。

加快保全和部分披露流量数据

对于前一条规定要保全的流量数据：

(a) 确保快速保全流量数据，无论通信传输涉及一个还是多个服务提供者；

(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，以便该缔约国能够确定服务提供者和通信传输路径。

[12] 资料来源：中国和俄罗斯联邦的提案。

提交令

各缔约国均应采取必要措施，授权其国内主管机关命令其境内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。

搜查和扣押已存储的计算机数据

1. 各缔约国均应采取必要措施，授权其国内主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及其中存储的计算机数据；

(b) 其境内可以存储计算机数据的计算机数据存储介质。

2. 各缔约国均应采取必要措施，使其国内主管机关能够将搜查或以类似方式访问快速扩展到另一系统，只要它们有理由认为所寻求数据存储在其境内另一计算机系统或其一部分中，而且可从初始系统中合法访问或取用此类数据，则其主管机关应当能够将搜查或以类似方式访问快速扩展到该另一系统。

3. 各缔约国均应采取必要措施，授权其国内主管机关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。这些措施包括有权：

(a) 扣押或以类似方式取得计算机系统或其一部分或计算机数据存储介质；

(b) 制作并留存这些计算机数据的副本；

(c) 维护相关所存储计算机数据的完整性；

(d) 使被访问的计算机系统中的计算机数据不可访问或移除。

4. 各缔约国均应采取必要措施，授权其国内主管机关命令任何了解计算机系统运行或为保护计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取第 1 款和第 2 款所述的措施。

管辖权

1. 各缔约国均应采取必要措施，在下列情况下对本公约中所定犯罪确立其管辖权：

(a) 犯罪发生在该缔约国境内；

(b) 犯罪发生在犯罪时悬挂该缔约国国旗的船只上或已根据该缔约国本国法律注册的航空器内；或者

(c) 犯罪者为该缔约国国民或在其境内有惯常居所的无国籍人。

2. 使缔约国能够在被指控犯罪的人在其境内并且只因该人为其国民不予以引渡时，对依本公约确定的犯罪确立其管辖权。

3. 使一缔约国能够在被指控犯罪的人在其境内并且不予以引渡时，对依本公约确定的犯罪确立其管辖权。

4. 如果根据第 1 款或第 2 款行使管辖权的缔约国被告知或通过其他途径获悉，任何其他缔约国正在对同一行为进行调查、起诉或审判程序，这些缔约国的主管机关应酌情相互磋商，以便协调行动。

5. 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依据其国内法确立的任何刑事管辖权。

哥伦比亚

[原文：西班牙文]
[2022 年 4 月 8 日]

程序措施和执法

考虑到在《联合国打击跨国有组织犯罪公约》、《联合国反腐败公约》和《布达佩斯网络犯罪公约》所确立的权力和程序方面对哥伦比亚有约束力的条款，就程序措施和执法提出以下相应条款：

措施	现有国际文书的条款
权力和程序	《布达佩斯公约》第 14 条
条件和保障措施	《布达佩斯公约》第 15 条
加快保全已存储的计算机数据	《布达佩斯公约》第 16 条
加快保全和部分披露流量数据	《布达佩斯公约》第 17 条
提交令	《布达佩斯公约》第 18 条
搜查和扣押已存储的计算机数据	《布达佩斯公约》第 19 条
实时收集流量数据	《布达佩斯公约》第 20 条
拦截内容数据	《布达佩斯公约》第 21 条
管辖权	《布达佩斯公约》第 22 条、《有组织犯罪公约》第十五条和《反腐败公约》第四十二条
冻结、扣押和没收	《反腐败公约》第三十一条

埃及

[原文：阿拉伯文]
[2022 年 4 月 8 日]

第三章 刑事诉讼和执法

建议本章包括以下三个主要条款：

第 31 条 程序问题的范围

1. 各缔约国应采取必要的立法措施，确立权力和程序，以预防、识别、侦查和调查犯罪和其他非法行为，并进行相关的审判程序。

2. 各缔约国应将上述权力和程序适用于：

(a) 本公约所列的刑事犯罪和其他非法行为；

(b) 利用信息和通信技术实施的其他刑事犯罪和其他非法行为；

(c) 收集电子证据。

第 32 条 刑事诉讼

刑事诉讼应包括：

1. 迅速保全存储在信息和通信技术中的数据，包括存储在信息技术的用户跟踪信息，特别是在认为此类信息可能会丢失或被修改之时，可发布命令，责成有关人员保全其拥有或控制的此类数据的完整性，以便使主管机关能够搜查和调查，同时对这方面采取的任何行动保密。

2. 迅速保存和部分披露用户跟踪信息，无论有多少服务提供者参与此类信息的传输，并确保主管机关迅速披露大量流量数据，使缔约国能够识别服务提供者和通信传输路径。

3. 命令提供由缔约国境内的个人拥有并存储在信息技术或存储介质上的信息，或由在缔约国境内提供服务的服务提供者掌握或控制的信息。

4. 检查存储的信息或访问存储在信息技术或存储介质上的信息。

5. 扣押、复制和保留存储的信息，以便执行搜查和访问该信息的程序。

6. 实时收集用户跟踪信息，责成缔约国管辖范围内的服务提供者收集、记录此类信息并保持其保密性。

7. 拦截内容信息，使主管机关能够用技术手段实时收集和记录通过信通技术传输的信息。

8. 各缔约国应采取必要的立法和其他措施，使其主管机关能够制止传播和广播任何构成本公约所列犯罪的内容。

第 33 条. 采纳数字证据

从装置、设备、电子媒体、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数字证据，在符合缔约国法律规定的技术条件时，应具有刑事证据中重大法证证据的证明价值。

萨尔瓦多

[原文：西班牙文]
[2022 年 4 月 12 日]

程序措施和执法

程序措施的范围

各缔约国均应采取必要的立法和其他措施，确立本节规定的权力和程序，以便进行具体刑事侦查或诉讼。

除非另有明确规定，否则各缔约国均应将本条上一款所述权力和程序用于：

(a) 根据本公约条款确立的犯罪；

(b) 借助计算机系统实施的其他刑事犯罪；

(c) 收集刑事犯罪的电子证据。

条件和保障措施

各缔约国应确保本节所规定的权力和程序的确立、实施和适用符合其国内法规定的条件和保障措施，这些条件和保障措施应充分保护人权和自由。

鉴于有关程序或权力的性质，此类条件和保障措施除其他外还应酌情包括司法或其他独立监督、适用的正当理由以及此类权力或程序范围和期限的限制。

在符合公共利益，特别是健全司法的范围内，各缔约国均应考虑本节规定的权力和程序对第三方权利、责任和合法利益的影响。

索取犯罪信息的权力

各缔约国均应采取必要的立法和其他措施，授权其主管机关命令或以类似方式迫使其境内的自然人或法人提交由其掌握或控制的、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。

保全存储在计算机系统中的数据

各缔约国应采取必要的立法和其他措施，使其主管机关能够下令或以类似方式实现快速保全通过计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或被修改的情况下。

如果缔约国实施上款规定，命令某人保全其拥有或控制的特定存储计算机数据，则该缔约国应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护这些计算机数据的完整性，最长不超过 90 天，以便主管机关能够寻求披露这些数据。缔约国可以规定此种命令嗣后可延期。

各缔约国应采取必要的立法和其他措施，责成保管人或其他负责保全计算机数据的人在其本国法律规定的期限内对采取此类程序事宜保密。

搜查和扣押已存储的计算机数据

各缔约国应采取必要的立法和其他措施，授权其主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及存储在其中的计算机数据；

(b) 在其领土内可能存储计算机数据的计算机数据存储介质。

各缔约国应采取必要的立法和其他措施，确保若其主管机关根据第 1 款(a)项搜查或以类似方式访问某一特定计算机系统或其一部分，并有理由认为所找数据存储在其领土内的另一计算机系统或其一部分中，且可从初始系统合法访问或取用此类数据，则其主管机关应能迅速将搜查或类似访问扩大到该另一系统。

各缔约国应采取必要的立法和其他措施，授权其主管机关扣押或以类似方式获取根据前几款规定访问的计算机数据。这些措施应包括以下权力：

(a) 扣押或以类似方式获取计算机系统或其一部分或计算机数据存储介质；

(b) 制作并保留这些计算机数据的副本；

(c) 维护相关所存储计算机数据的完整性；

(d) 使被访问的计算机系统中的那些计算机数据不可访问或移除。

各缔约国应采取必要的立法和其他措施，授权其主管机关命令任何了解计算机系统运行或为保护系统中的计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取前几款所述的措施。

实时收集流量数据

各缔约国应采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国领土上应用技术手段收集或记录；

(b) 迫使服务提供者在其现有技术能力范围内：在该缔约国领土上应用技术手段收集或记录；或者配合并协助主管机关实时收集或记录与其境内借助计算机系统传输的指定通信相关的流量数据。

如果一个缔约国由于其国内法律制度的既定原则而不能采取第 1 款(a)项所述的措施，它可以采取必要的立法和其他措施，确保在其领土上应用技术手段，实时收集或记录与在其领土上传输的指定通信有关的流量数据。

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

拦截内容数据

各缔约国应当对将由本国法律确定的一系列严重犯罪采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国领土上应用技术手段收集或记录；

(b) 迫使服务提供者在其现有技术能力范围内：在该缔约国领土上应用技术手段收集或记录；或者配合并协助主管机关实时收集或记录与其境内借助计算机系统传输的指定通信相关的内容数据。

如果一个缔约国由于其国内法律制度的既定原则而不能采取第 1 款(a)项所述的措施，它可以采取必要的立法和其他措施，确保在其领土上应用技术手段，实时收集或记录与在其领土上传输的指定通信有关的流量数据。

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

没收和冻结

缔约国应在本国法律制度的范围内尽最大可能采取必要措施，以便能够没收：

(a) 本公约所涵盖犯罪产生的犯罪所得或价值与其相当的财产；

(b) 用于或拟用于本公约所涵盖的犯罪的财产、设备或其他工具。

缔约国应采取必要措施，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。

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，则应将此类财产视为犯罪所得的替代财产，适用本条所述措施。

如果犯罪所得已与从合法来源获得的财产相混合，则应在不影响冻结权或扣押权的情况下没收这类财产，没收价值可达混合于其中的犯罪所得的估计价值。

对于来自犯罪所得、来自由犯罪所得转变或转化而成的财产或已与犯罪所得相混合的财产的收入或其他利益，也应适用本条所述措施，其方式和程度与处置犯罪所得相同。

各缔约国应授权其法院或其他主管机关命令提供或扣押银行、财务或商业记录。缔约国不得以银行保密为由拒绝按照本款规定采取行动。

缔约国可考虑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本国法律原则和司法及其他程序的性质。

不得对本条规定作损害善意第三方权利的解释。

本条任何规定均不得影响本条所述措施应根据缔约国本国法律规定予以确定和实施的原则。

没收的犯罪所得或财产的处置

缔约国依照本公约没收的犯罪所得或财产应由该缔约国根据其国内法和行政程序予以处置。

根据本公约应另一缔约国的请求采取行动时，缔约国应在本国法律允许的范围内，根据请求，优先考虑将没收的犯罪所得或财产交还请求缔约国，以便其对犯罪被害人进行赔偿，或将这类犯罪所得或财产归还其合法所有人。

根据本公约规定应另一缔约国的请求采取行动时，缔约国可特别考虑就下列事项缔结协定或安排：

(a) 将这类犯罪所得或财产的价款，或变卖这类犯罪所得或财产所得的款项，或这类款项的一部分捐给根据本公约规定指定专门打击有组织犯罪的政府间机构确定的账户；

(b) 根据其国内法或行政程序，经常或逐案与其他缔约国分享这种犯罪所得或财产，或变卖这种犯罪所得或财产所得款项。

建立犯罪记录

各缔约国均可采取必要的立法或其他措施，按其认为适宜的条件并为其认为适宜的目的，考虑另一国以前对被指控犯罪人所作的任何有罪判决，以便在涉及本公约所涵盖犯罪的刑事诉讼中使用这种信息。

保护证人

各缔约国均应在其力所能及的范围内采取适当的措施，为刑事诉讼中就本公约所涵盖的犯罪作证的证人并酌情为其亲属及其他与其关系密切的人提供有效的保护，使其免遭可能的报复或恐吓。

在不影响被告人的权利包括正当程序权的情况下，本条前款所述措施可包括：

(a) 制定向此种人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限制披露有关其身份和下落的情况；

(b) 规定可允许证人以确保其安全的方式作证的证据规则，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。

(c) 缔约国应考虑与其他国家订立有关转移本条第 1 款所述人员的安排。

(d) 本条的规定也应适用于作为证人的被害人。

帮助和保护被害人

各缔约国均应在其力所能及的范围内采取适当的措施，以便向本公约所涵盖的犯罪的被害人提供帮助和保护，尤其是在其受到报复威胁或恐吓的情况下。

各缔约国均应制定适当的程序，使本公约所涵盖的犯罪的被害人有机会获得赔偿和补偿。

各缔约国均应在符合其本国法律的情况下，在对犯罪人提起的刑事诉讼的适当阶段，以不损害被告人权利的方式使被害人的意见和关切得到表达和考虑。

加强与执法机关合作的措施

各缔约国均应采取适当措施，鼓励参与或曾参与有组织犯罪集团的人：

(a) 为主管机关的侦查和取证提供有用信息，例如：

㈠ 犯罪集团和组织的身份、性质、组成情况、结构、所在地或活动；

㈡ 与其他有组织犯罪集团之间的联系，包括国际联系；

㈢ 有组织犯罪集团所实施或可能实施的犯罪；

(b) 向主管机关提供可能有助于剥夺有组织犯罪集团的资源或犯罪所得的实际而具体的帮助。

对于在侦查或起诉本公约所涵盖犯罪时予以实质性配合的被告人，各缔约国均应考虑规定在适当情况下减轻处罚的可能性。

对于本公约所涵盖的犯罪的侦查或起诉中予以实质性配合者，各缔约国均应考虑根据其本国法律基本原则规定允许免予起诉的可能性。

应按本公约相应条款的规定为此类人员提供保护。

如果本条第 1 款所述的、位于一缔约国的人员能给予另一缔约国主管机关以实质性配合，有关缔约国可考虑根据其本国法律订立关于由对方缔约国提供本条第 2 款和第 3 款所列待遇的协定或安排。

欧洲联盟及其成员国

[原文：英文]
[2022 年 4 月 6 日]

第三章
刑事程序和执法

第 13 条
程序措施的范围

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

2. 各缔约国应将本条第 1 款所述权力和程序适用于：

(a) 根据本公约第 5 条至第 10 条确定的刑事犯罪；

(b) 收集根据本公约第 5 条至第 10 条确定的刑事犯罪的电子形式的证据。

第 14 条
条件和保障措施

1. 各缔约国应确保本章所规定权力和程序的确立、实施和适用遵守其国内法规定的条件和保障措施，其中应规定根据国际人权标准，充分全面保护人权和基本自由，包括根据其依据《世界人权宣言》、《公民及政治权利国际公约》、《禁止酷刑和其他残忍、不人道或有辱人格的待遇或处罚公约》、《儿童权利公约》、《儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》和其他国际人权文书所承担义务产生的权利，还应纳入相称性、合法性和必要性原则并且保护隐私和个人数据。

2. 鉴于有关程序或权力的性质，此类条件和保障措施除其他外还应酌情纳入司法或其他独立监督、适用的正当理由以及此类权力或程序的范围和期限限制。

3. 在符合公共利益、特别是健全司法的范围内，各缔约国应考虑本章规定的权力和程序对第三方权利、责任和合法利益的影响。

第 15 条
加快保全已存储的计算机数据

1. 各缔约国均应采取必要措施，使其主管机关能够下令或以类似方式实现快速保全特定计算机数据，包括借助计算机系统存储的流量数据，特别是在有理由认为计算机数据特别容易丢失或被修改的情况下。

2. 如果缔约国为执行上文第 1 款，命令某人保全其拥有或控制的指定已存储计算机数据，则该缔约国应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护计算机数据的完整性，最长不超过 90 天，以便主管机关能够寻求披露这些数据。缔约国可规定此种命令嗣后可以延期。

3. 各缔约国均应采取必要的立法和其他措施，责成监管人或负责保全计算机数据的其他人在本国法律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受第 14 条和第 15 条的约束。

第 16 条
提交令

1. 各缔约国均应采取必要措施，授权其主管机关下令：

(a) 其境内的个人提交其拥有或控制的、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；

(b) 缔约国境内提供服务的服务提供者提交其拥有或控制的与这类服务有关的用户信息。

2. 本条所述权力和程序应受第 14 条和第 15 条的约束。

第 17 条
搜查和扣押已存储的计算机数据

1. 各缔约国均应采取必要措施，授权其主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及其中存储的计算机数据；

(b) 其境内可以存储计算机数据的计算机数据存储介质。

2. 各缔约国均应采取必要措施，确保如其主管机关根据第 1 款(a)项搜查或以类似方式访问某一特定计算机系统或其一部分，并有理由认为所寻求数据存储在其境内另一计算机系统或其一部分中，而且这种数据可从初始系统中合法获取或供初始系统使用，主管机关应当能够快速将搜查或类似访问扩展到该另一系统。

3. 各缔约国均应采取必要的立法和其他措施，授权其主管机关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。这些措施应包括有权：

(a) 扣押或以类似方式取得计算机系统或其一部分或计算机数据存储介质；

(b) 制作并留存这些计算机数据的副本；

(c) 维护相关的所存储计算机数据的完整性；

(d) 使被访问的计算机系统中的计算机数据不可访问或移除。

4. 各缔约国均应采取必要的立法和其他措施，授权其主管机关命令任何了解计算机系统运行或为保护其中的计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取第 1 款和第 2 款所述措施。

5. 本条所述权力和程序应受第 14 条和第 15 条的约束。

第 18 条
管辖权

1. 各缔约国均应采取必要措施，在下列情况下，对根据本公约第 5 条至第 10 条确定的犯罪确立管辖权：

(a) 犯罪发生在该缔约国境内；

(b) 犯罪发生在犯罪时悬挂该缔约国国旗的船只上或发生在根据该缔约国法律注册的航空器内；或者

(c) 犯罪系由其国民所实施，条件是该犯罪行为根据犯罪发生地的刑法应受到惩罚，或者实施犯罪是在任何缔约国领土管辖范围之外。

2. 在下列情况下，各缔约国也可以对任何这类犯罪确立其管辖权：

(a) 犯罪系针对该缔约国国民；

(b) 犯罪者为该缔约国国民或在其境内有惯常居所的无国籍人。

3. 各缔约国也可以采取必要措施，当被指控犯罪人在本国境内、在收到引渡请求后只以其国籍为依据不予以引渡时，对本公约所涵盖犯罪确立其管辖权。

4. 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通过其他途径获悉，一个或多个其他缔约国正在对同一行为进行侦查、起诉或审判程序，这些缔约国的主管机关应酌情相互磋商，以便协调行动。

5. 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依据本国法律确立的任何刑事管辖权。

第 19 条
帮助和保护被害人

1. 各缔约国应在其力所能及的范围内采取适当措施，为根据本公约第 5 条至第 10 条确定的犯罪的被害人提供援助和保护。

2. 各缔约国应制定适当的程序，为根据本公约第 5 条至第 10 条确定的犯罪的被害人提供获得赔偿的机会。

3. 各缔约国应在不违背本国法律的情况下，在对犯罪人提起刑事诉讼的适当阶段，以不损害被告人权利的方式，使被害人的意见和关切得到表达和考虑。

加纳

[原文：英文]
[2022 年 4 月 12 日]

第三章
程序措施和执法[13]

第 23 条 程序规定的范围

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

2. 除非另有明确规定，各缔约国应将本条第 1 款所述权力和程序应用于：

(a) 根据本公约第 5 条至第 20 条确定的刑事犯罪；

(b) 借助计算机系统实施的其他刑事犯罪；

(c) 收集刑事犯罪的电子形式的证据。

3. 各缔约国可保留将第 29 条所述措施仅适用于保留意见中具体所指罪行或罪行类别的权利，条件是这些罪行或罪行类别的范围不得比缔约国适用第 30 条所述措施的罪行范围更严格。各缔约国应考虑限制这类保留，以使第 29 条所述措施能得到最广泛的适用。

[13] 本节的案文主要摘自《布达佩斯公约》、《非洲联盟网络安全和个人数据保护公约》、2008 年《电子交易法》（《第 772 号法》）和 2020 年《网络安全法》（《第 1038 号法》）。这些文书构成加纳的网络犯罪立法框架。

4. 如果缔约国由于本公约通过时其现行立法的限制，无法将第 29 条和第 30 条所述措施适用于服务提供者的计算机系统内传输的通信，该系统：

(a) 运营是为了某一封闭用户群体获利；

(b) 不使用公共通信网络，也不与另一公共或私人计算机系统连接，则该缔约国可保留对这类通信不适用这些措施的权利。各缔约国应考虑限制这类保留，以使第 29 条和第 30 条所述措施能得到最广泛的适用。

5. 如果缔约国由于本公约通过时其现行立法的限制，无法适用第 31 条所述措施，则该缔约国可保留不适用这些措施的权利。各缔约国应考虑限制此种保留，以使第 31 条所述措施能得到最广泛的适用。

第 24 条 条件和保障措施

1. 各缔约国应确保本节所规定权力和程序的确立、实施和适用遵守其根据本国法律规定的条件和保障措施，其中应规定充分保护人权和自由，包括其依《国际人权宪章》，[14]包括《世界人权宣言》和《公民及政治权利国际公约》以及其他适用的国际人权文书所承担义务而产生的权利，应纳入相称性和必要性原则，并确保司法监督。

2. 鉴于有关程序或权力的性质，此类条件和保障措施除其他外还应酌情纳入司法或其他独立监督、适用的正当理由以及此类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，各缔约国应考虑本节规定的权力和程序对第三方的权利、责任和合法利益的影响。

第 25 条 加快保全已存储的计算机数据[15]

1. 各缔约国均应采取必要的立法和其他措施，使其主管机关能够下令或以类似方式实现快速保全借助计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或被修改的情况下。

2. 如果缔约国执行上文第 1 款，命令某人保全其拥有或控制的指定已存储计算机数据，侧该缔约方应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护该计算机数据的完整性，最长不超过 90 天，以便主管机关能够寻求披露这些数据。缔约国可规定此种命令嗣后可以延期。

3. 各缔约国均应采取必要的立法和其他措施，责成保管人或其他负责保全计算机数据的人在其国内法规定的期限内对采取这类程序事宜保密。

4. 本条所述权力和程序应受第 19 条和第 20 条的约束。

---

[14] 联合国人权事务高级专员办事处，“国际人权法”（www.ohchr.org/zh/instruments-and-mechanisms/international-human-rights-law）。

[15] 与《布达佩斯公约》、《非洲联盟网络安全和个人数据保护公约》和加纳 2008 年《电子交易法》（《第 772 号法》）和 2020 年《网络安全法》（《第 1038 号法》）相一致。

第 26 条 加快保全和部分披露流量数据[16]

1. 对于应根据第 21 条予以保全的流量数据，各缔约国均应采取必要的立法和其他措施，以便：

(a) 确保快速保全这种流量数据，无论该通信传输涉及一个还是多个服务提供者；

(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，以便该缔约国能够确定服务提供者和通信传输路径。

2. 本条所述权力和程序应受第 23 条和第 24 条的约束。

第 27 条 提交令

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关命令：

(a) 本国境内的个人提交其拥有或控制的、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；

(b) 缔约国境内提供服务的服务提供者提交其拥有或控制的与这类服务有关的用户信息。

2. 各缔约国均应采取必要的立法和其他措施，确保计算机数据或用户信息的提交令只由相关主管机关在司法机关等独立监督实体的监督下获得。这类措施应确保要求主管机关向独立监督机关令其确信地证明，有合理的理由认为与被调查者有关的计算机数据或用户信息是进行特定刑事侦查合理需要的。

3. 为了第 2 款之目的，主管机关应：

(a) 向独立监督机关说明主管机关为什么认为所寻求计算机数据或用户信息将：

㈠ 供控制或拥有计算机数据或计算机系统的人使用；或者

㈡ 供相关的服务提供者使用；

(b) 确定并具体说明所寻求计算机数据或用户信息的类型；

(c) 指明应采取哪些措施确保获得用户信息或计算机数据；

㈠ 同时维护其他用户、客户和第三方的隐私；

㈡ 不披露未构成调查对象的任何一方的用户信息或计算机数据。

4. 各缔约国均应采取必要的立法和其他措施，确保独立监督机关可根据第 2 款准予提交令，如果它确信：

(a) 索要的信息对于特定刑事侦查或起诉而言是相当、相称和必要的；

(b) 应采取措施，确保在执行命令的同时，维护其他用户、客户和第三方的隐私，并且不泄露未构成调查对象的任何一方的信息和数据；

[16] 与《布达佩斯公约》相一致。

(c) 除非允许提交信息，否则调查可能会受阻或受到严重损害。

5. 本条所述权力和程序应受第 23 条和第 24 条的约束。

6. 就本条而言，“用户信息”一词是指服务提供者掌握的以计算机数据形式或任何其他形式存储的除流量数据或内容数据之外与其服务用户有关的任何信息，，通过这些信息可以确定：

(a) 使用的通信服务类型、对其采用的技术条件和服务期限；

(b) 根据服务协议或安排可获得的用户身份、邮政或地理地址、电话和其他联系号码、账单和付款信息；

(c) 根据服务协议或安排可获得的关于通信设备安装地点的任何其他信息。

第 28 条 搜查和扣押已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及其中存储的计算机数据；

(b) 本国境内可以存储计算机数据的计算机数据存储介质。

2. 各缔约国均应采取必要的立法和其他措施，确保如其主管机关根据第 1 款(a)项搜查或以类似方式访问某一特定计算机系统或其一部分，并有理由认为所寻求数据存储在其境内另一计算机系统或其一部分中，且这类数据可从初始系统合法获取或供初始系统使用，主管机关应当能够快速地将搜查或类似访问扩展到该另一系统。

3. 各缔约国均应采取必要的立法和其他措施，授权其主管机关扣押或以类似方式取得根据第 1 款或第 2 款获取的计算机数据。这些措施应包括有权：

(a) 扣押或以类似方式取得计算机系统或其一部分或计算机数据存储介质；

(b) 制作并留存该计算机数据的副本；

(c) 维护相关的所存储计算机数据的完整性；

(d) 使被访问的计算机系统中的计算机数据不可访问或移除。

4. 各缔约国均应采取必要的立法和其他措施，授权其主管机关命令任何了解计算机系统运行或为保护计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取第 1 款和第 2 款所述措施。

5. 各缔约国均应采取必要的立法和其他措施，授权其主管机关由一名获得授权者陪同，并有权在该人协助下，能采取第 1 款、第 2 款和第 3 款所述措施。

6. 各缔约国均应采取必要的立法和其他措施，授权其主管机关在根据其国内法执行搜查令时，扣押任何计算机、电子记录、程序、信息、文件或物品，条件是主管机关有合理理由认为根据本公约第 1 条至第 16 条确定的任何犯罪已经或将要实施。

7. 本条所述权力和程序应受第 23 条和第 24 条的约束。

第 29 条 实时收集流量数据

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国境内用技术手段实时收集或记录；

(b) 迫使服务提供者在其现有的技术能力范围内：

㈠ 在该缔约国境内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其境内借助计算机系统传输的特定通信相关的流量数据。

2. 各缔约国均应采取必要的立法和其他措施，确保本条规定的权力只能由相关主管机关在司法机关等独立监督实体的监督下获得。这类措施应确保要求主管机关向独立监督机关令其确信地证明，有合理的理由认为与被调查者有关的流量数据是进行特定刑事调查合理需要的。

3. 为了第 2 款之目的，主管机关应：

(a) 向独立监督机关说明为什么主管机关认为所寻求流量数据将：

㈠ 供控制或拥有计算机系统的人使用；或者

㈡ 供服务提供者使用；

(b) 确定并具体说明正在寻求的流量数据类型；

(c) 确定并具体说明寻求本条所规定权力针对的犯罪；

(d) 指明应采取哪些措施确保获得流量数据：

㈠ 同时维护其他用户、客户和第三方的隐私；

㈡ 不披露不属于调查对象的任何一方的流量数据。

4. 各缔约国均应采取必要的立法和其他措施，确保独立监督机关可授予实时收集流量数据的权力，条件是独立监督机关确信：

(a) 拦截程度对于特定刑事侦查或起诉而言是相当、相称和必要的；

(b) 应采取措施，确保在行使权力的同时维护其他用户、客户和第三方的隐私，并且不泄露未构成调查对象的任何一方的信息和数据；

(c) 除非授予了实时收集流量数据的权力，否则调查可能会受阻或受到严重损害。

5. 如果缔约国由于其本国法律制度的既定原则无法采取第 1 款(a)项所述措施，该缔约国可以采取必要的立法和其他措施，确保在其境内用技术手段，实时收集或记录与其境内传输的指定通信有关的流量数据。

6. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条所规定的任何权力的事实以及与此有关的任何信息保密。

7. 本条所述权力和程序应受第 23 条和第 24 条的约束。

第 30 条 拦截内容数据

1. 各缔约国应对本国法律所确定的一系列严重犯罪采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国境内用技术手段实时收集或记录；

(b) 迫使服务提供者在其现有的技术能力范围内：

㈠ 在该缔约国境内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其境内借助计算机系统传输的指定通信的内容数据。

2. 各缔约国均应采取必要的立法和其他措施，确保本条规定的权力只由相关主管机关在司法机关等独立监督实体的监督下获得。这类措施应确保要求主管机关向独立监督机关令其确信地证明，有合理的理由授权为以下任一目的拦截与接受刑事调查的人员或场所有关或有联系的内容数据：

(a) 国家安全利益；

(b) 防止或侦查严重罪行；

(c) 维护公民的经济利益，只要这些利益也与国家安全利益相关；或者

(d) 执行司法协助请求。

3. 为了第 2 款之目的，主管机关应：

(a) 向独立监督机构说明为什么主管机关认为所寻求内容将：

㈠ 供控制或拥有计算机系统的人使用；

㈡ 供服务提供者使用；

(b) 确定并说明疑似在计算机系统中发现的或为服务提供者拥有或控制的内容数据类型；

(c) 确定并具体说明寻求本条所规定权力针对的罪行；

(d) 指明应采取哪些措施确保获取内容数据：

㈠ 同时维护其他用户、客户和第三方的隐私；

㈡ 不披露不属于调查对象的任何一方的流量数据。

4. 各缔约国均应采取必要的立法和其他措施，确保独立监督机关可授予拦截内容数据的权力，条件是独立监督机关确信：

(a) 拦截程度对于特定刑事调查或起诉而言是相当、相称和必要的；

(b) 应采取措施，确保在行使拦截内容数据权力的同时，维护其他用户、客户和第三方的隐私，并且不披露不属于调查对象的任何一方的信息和数据；

(c) 除非准许拦截，否则调查可能受阻或受到严重损害。

5. 如果缔约方由于其本国法律制度的既定原则无法采取第 1 款(a)项所述措施，该缔约国可以采取必要的立法和其他措施，确保在其境内用技术手段，实时收集或记录其境内指定通信的内容数据。

6. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条所规定的任何权力的事实以及与此相关的任何信息保密。

7. 本条所述权力和程序应受第 23 条和第 24 条的约束。

第 31 条 留存数据

1. 各缔约国均应采取必要的立法和其他措施，保证其境内的服务提供者留存：

(a) 用户信息至少六年；

(b) 流量数据 12 个月。

2. 本条所述权力和程序应受第 23 条和第 24 条的约束。

3. 如果缔约国由于本公约通过时其现行立法的限制无法适用本条所述措施，该缔约国可保留不适用这些措施的权利。各缔约国应考虑限制此种保留，使本条所述措施能得到最广泛的应用。

第 32 条 没收和扣押

1. 各缔约国应在本国的法律制度范围内尽最大可能采取必要措施，以便能够没收：

(a) 本公约所涵盖犯罪产生的犯罪所得或价值与其相当的财产；

(b) 用于或拟用于本公约所涵盖犯罪的财产、设备或其他工具。

2. 各缔约国均应采取必要措施，辨认、追查、冻结或扣押本条第 3 款所述任何物品，以便最终予以没收。

3. 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，则应当将此类财产视为犯罪所得的替代财产，适用本条所述措施。

4. 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。

5. 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，其方式和程度与处置犯罪所得相同。

6. 为了本条之目的，各缔约国应授权其法院或其他主管机关下令提供或扣押银行、财务或商业记录。各缔约国不得以银行保密为由拒绝根据本款的规定采取行动。

7. 各缔约国可以考虑，在要求符合其本国法律原则以及司法和其他程序的性质的情况下，能否要求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。

8. 不得对本条规定作损害善意第三方权利的解释。

9. 本条任何规定均不得影响本条所述措施应根据且遵照缔约国本国法律规定予以确定和实施的原则。

第 33 条 管辖权

1. 各缔约国均应采取必要的立法和其他措施，在下列情况下，对根据本公约第 5 条至第 20 条确定的任何犯罪确立管辖权：

(a) 犯罪发生在该缔约国境内，或者

(b) 犯罪发生在悬挂该缔约国国旗的船只上；或者

(c) 犯罪发生在根据该缔约国法律注册的航空器内；或者

(d) 犯罪系由其国民所实施，条件是该犯罪行为根据犯罪实施地所在国的刑法应受到惩罚，或者实施犯罪是在任何缔约国领土管辖范围之外。

2. 各缔约国可保留不适用或仅在特定情况或条件下适用本条第 1 款(b)项至(d)项或其任何部分规定的管辖权规则的权利。

3. 为了本公约引渡条款之目的，各缔约国均应采取必要措施，当被指控犯罪人在本国境内、在收到引渡请求后只以其国籍为依据不将其引渡到另一缔约国时，对根据本公约确定的罪行确立管辖权。

4. 本公约不排除缔约国根据其本国法律行使的任何刑事管辖权。

5. 当不止一个缔约国声称对根据本公约确定的某项被控犯罪的管辖权时，所涉缔约国应酌情进行协商，以期确定最合适的起诉管辖权。

伊朗伊斯兰共和国

[原文：英文]
[2022 年 4 月 8 日]

3. 执法和程序措施

罪犯滥用服务提供者和社交媒体网络平台等私营部门所提供服务的现象由来已久且愈演愈烈。这构成了一项令人生畏的挑战，需要采取具体的对策。在调查和起诉此类犯罪以及制止此类滥用方面，上述实体与执法实体的合作是至关重要的，有鉴于此，该公约应就私营部门、服务提供者和其他类似实体（特别是在国际一级开展全球性或大量活动的部门和服务提供者）与执法机关的合作规定具体的义务和条例。

有效确保这些实体与执法和司法机关进行及时、有效合作的措施应构成该公约的一个组成部分。为此，应通过公约内的具体章节，处理国家机关与服务提供者

和私营部门等实体之间的合作问题，并确定具体措施，包括快速保全电子数据并向执法实体披露。

由于电子证据是调查和起诉使用信息和通信技术实施的犯罪的重要因素，因此该公约规定的程序需要包括获取、维护和披露真实电子证据的标准化流程。标准程序可以确保各缔约国在国家一级协调一致应对此类犯罪，也能确保各缔约国的执法和司法机关在国际一级就保全和提供电子证据进行更有效的合作。

追回和返还资产和犯罪所得在消除罪犯实施犯罪的动机和减少累犯，以及赔偿受害者方面发挥重要作用。因此，快速扣押、追回和返还犯罪所得应构成该公约的一项关键内容。公约中与执法和程序措施相关的条款应赋予国家机关权力，以确保顺利和快速追回资产和犯罪所得，并且在这一领域采取最广泛的援助与合作措施。

打击将信息和通信技术用于犯罪目的，要求执法实体在调查和起诉犯罪过程中相应地配备和使用现代技术，以应对此类犯罪。因此，应鼓励促进和支持执法和司法机关使用现代技术，包括在防止和打击借助信息和通信技术实施犯罪方面的全部程序措施中使用现代技术。这也需要通过政治中立和可靠的技术援助向执法和司法机关提供必要的设备和技术。

日本

[原文：英文]
[2022 年 4 月 8 日]

3. 程序措施和执法

3.1 关于网络犯罪调查的程序措施，可以考虑规定快速保全、搜查和扣押已存储的计算机数据，提交令和实时收集流量数据。

3.2 我们可以考虑将这些程序规定适用于本公约确立的刑事犯罪和其他使用计算机系统所实施犯罪的调查和刑事诉讼，适用于收集刑事犯罪的电子形式的证据。

3.3 在授予每个会员国主管机关上述权力时，有必要制定条款，确认每个会员国应确保适当保护因依照人权条约和其他文书所规定的义务而产生的权利以及其他人权和自由，并确保遵守包括相称性原则的国内立法。本公约应在有关程序措施和执法的章节中确认这一概念。

墨西哥

[原文：英文]
[2022 年 4 月 13 日]

程序措施和执法

鉴于数字证据对调查、起诉和执法的重要性，因此期望本公约的缔约国就得到普遍和最低限度确认的获取、处理和保全数字证据的程序措施达成一致。可增加

以下内容：“为调查目的或（和）收集证据和保全电子证据，各国可考虑并利用现有国际文书（如《联合国打击跨国有组织犯罪公约》）中的所有规定。”

关于提供信息和通信技术服务的私营实体，墨西哥建议纳入以下条款：

“缔约国承诺，使在其本国境内成立或在其国家管辖下运营的提供信息和通信技术服务的私营实体采取并执行尽职调查政策和程序，以避免对第三方造成损害。”

“缔约国还承诺，采取适当措施，确保在其本国境内成立或在其国家管辖下运营的私营实体不违反其他缔约国的法律。”

此外，公约中还应普遍呼吁提供信息和通信技术服务的私营实体在尊重适用的隐私条例的同时，就调查和起诉网络犯罪与国家执法和司法机关进行有效合作。

新西兰

[原文：英文]
[2022 年 4 月 8 日]

有关程序和执法措施的规定

10. 在纳入全面保障措施以确保保护人权和基本自由、尊重法治和恪守相称性原则的前提下，新西兰支持在本公约中纳入能够快速保全和访问数字证据的规定。例如，与以下几方面有关的规定：

- 搜查和扣押所要查找和相关的已存储的计算机数据
- 实时收集所要查找和相关的计算机数据
- 拦截所要查找和相关的计算机数据
- 保全所要查找和相关的计算机数据
- 索求个人拥有或控制的、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的提交令。

11. 新西兰还支持纳入确保罪犯无法通过其犯罪行为获利的规定，如扣押和没收犯罪所得，以及加强与执法机关合作的规定。

挪威

[原文：英文]
[2022 年 4 月 8 日]

程序措施和执法

9. 特设委员会应借鉴《联合国打击跨国有组织犯罪公约》和《联合国反腐败公约》等现有条约的经验。同时，铭记这项新公约要应对的是现代网络犯罪的挑战，应要求会员国纳入专门针对电子证据的国内规定。此外，特设委员会应注意到，在

调查或起诉网络犯罪时，时间和效率至关重要。《公约》应允许合作收集和获取任何类型犯罪的电子证据，而不仅仅是网络犯罪。

10. 为避免不必要的重复工作，应充分利用和加强现有运作良好的沟通渠道和网络。

11. 必须处理私营部门的关键作用。

12. 应做好对受害者的援助和保护工作，以及对证人的保护工作。

13. 关于程序措施的规定必须符合正当程序并保护人权和基本自由。

俄罗斯联邦，还代表白俄罗斯、布隆迪、中国、尼加拉瓜和塔吉克斯坦

[原件：俄文]
[2022 年 4 月 7 日]

第 2 节

刑事诉讼和执法

第 31 条 程序规定的范围

1. 各缔约国均应采取必要的立法和其他措施，确立本节所设想的权力和程序，目的是预防、侦查、制止、揭露和起诉犯罪和其他违法行为，并就这些犯罪和行为进行审判程序。

2. 除本公约第 33 条另有规定外，各缔约国应将本条第 1 款所述权力和程序适用于：

(a) 依照本公约第 6 条至第 29 条确立的刑事犯罪和其他违法行为；

(b) 借助信息和通信技术实施的其他刑事犯罪和其他违法行为；

(c) 收集与实施刑事犯罪和其他违法行为有关的证据，包括电子证据。

3. (a) 各缔约国均可提出保留，声明其保留权利，只对保留中列明的刑事犯罪或刑事犯罪类别适用本公约第 38 条所述措施，但此等刑事犯罪或刑事犯罪类别的范围不得比该缔约国适用本公约第 33 条各项规定所述措施处理的刑事犯罪范围更有限。各缔约国应考虑限制此类保留的适用，以使本公约第 38 条规定的措施能够得到最广泛的适用；

(b) 若缔约国由于受到本公约通过时有效的国内立法所限，不能对服务提供者信息系统内传输的信息适用本公约第 33 条和第 38 条所述措施，而该信息系统：

㈠ 正在为一个封闭用户群的利益运行，

㈡ 不使用信息和电信网络，也不与其他信息系统连接，

则该缔约国可保留不对此类信息传输适用上述措施的权利。

第 32 条 条件和保障措施

1. 各缔约国均应确保本节规定的权力和程序的确立、实施和适用符合其国内立法规定的条件和保障，其中应确保充分保护人权和自由，包括因缔约国依据 1966 年 12 月 16 日《公民及政治权利国际公约》及其他适用国际人权文书承担的义务而产生的权利。

2. 鉴于有关权力和程序的性质，此类条件和保障措施除其他外还应包括司法监督或其他独立监督、适用的正当理由以及此种权力或程序的范围和期限限制。

3. 在符合公共利益的限度内，特别是在司法方面，缔约国应考虑本节规定的权力和程序对第三方权利、责任和合法利益的影响。

第 33 条 收集借助信息和通信技术传输的信息

1. 为打击本公约所涵盖并依据国内立法确定的犯罪，各缔约国均应采取必要的立法和其他措施，授权其主管机关：

(a) 应用技术手段，在该缔约国境内收集或记录借助信息和通信技术传输的信息；

(b) 在服务提供者拥有技术能力的限度内，责成服务提供者：

㈠ 应用技术手段，在该缔约国境内收集或记录借助信息和通信技术传输的包含内容数据的电子信息；或者

㈡ 配合并协助该缔约国的主管机关实时收集或记录在该缔约国境内借助信息和通信技术传输的包含内容数据的电子信息。

2. 若缔约国由于其国内法律制度的长期既定原则而不能采取本条第 1 款(a)项所述的措施，则可转而采取必要的立法和其他措施，确保在其境内应用技术手段，实时收集或记录在其境内借助信息和通信技术传输的包含内容数据的电子信息。

3. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条规定的任何权力以及与之相关的任何信息保密。

4. 本条所述权力和程序应符合本公约第 31 条和第 32 条的规定。

第 34 条 快速保全累积的电子信息

1. 各缔约国均应采取必要的立法和其他措施，使其主管机关能够下达适当命令或指示，或者通过类似手段，确保迅速保全特定电子信息，包括流量数据，特别是在有理由认为数据极易被删除、复制或修改的情况下，包括因其国内法律或服务提供者的服务条款规定的保留期期满而出现上述情况时。

2. 若缔约国实施本条第 1 款的规定，命令个人（包括法人）保全其拥有或控制的指定已存储信息，则应采取必要的立法和其他法律措施，责成该人在必要时但不超过该缔约国本国法律规定的期间内保全此类信息并维护信息完整性，以使主管机关能够寻求披露此种数据。缔约国可以规定，此种命令嗣后可以延期。

3. 各缔约国还应采取必要的立法和其他措施，责成负责保全信息的人在其国内立法规定的期间对执行此类程序事宜保密。

4. 本条所述权力和程序的确立应符合本公约第 31 条和第 32 条的规定。

第 35 条 快速保全和部分披露流量数据

1. 各缔约国均应就本公约第 34 条规定应予以保全的流量数据采取必要的立法和其他措施：

(a) 确保无论有多少服务提供者参与了相关信息的传输，都有可能迅速保全流量数据；

(b) 确保向缔约国本国主管机关迅速披露数量充分的流量数据，以便该相关缔约国能够查明服务提供者和所指信息的传输路径。

2. 本条所述权力和程序应符合本公约第 31 条和第 32 条的规定。

第 36 条 提交令

1. 为本公约第 31 条第 1 款所述之目的，各缔约国均应采取必要的立法和其他措施，授权本国主管机关：

(a) 命令本国境内人员提供其拥有或控制的指定电子信息；

(b) 命令在缔约国本国境内提供服务的服务提供者提交其拥有或控制的用户信息。

2. 本条所述权力和程序的确立应符合本公约第 31 条和第 32 条的规定。

3. 就本条目的而言，“用户信息”一词系指服务提供者掌握的除流量数据或内容数据之外与其服务用户有关的任何信息，基于这些信息有可能确定：

(a) 使用的信息和通信服务类型、对其采用的技术规定和服务期；

(b) 可从服务协议或安排中获取的用户身份、邮政地址或其他地址、电话和其他接入号码，包括互联网协议地址，以及账单和付款信息；

(c) 对服务协议或安排有影响的信息和通信设备的位置信息。

第 37 条 搜查和扣押以电子方式存储或处理的信息

1. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关寻求访问本国境内或受本国管辖的：

(a) 信通技术装置和其中存储的信息；

(b) 可能存储有所要查找的电子信息的信息存储介质。

2. 各缔约国均应采取必要的立法和其他措施，确保若本国主管机关在根据本条第 1 款(a)项的规定进行搜查时，有理由认为所查找的信息存储于其境内另一信息和

通信技术装置内，则该主管机关应能够迅速进行搜查，以得以访问该另一信息和通信技术装置或其中存储的数据。

3. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关扣押其境内或受其管辖的电子信息，或通过类似手段取得该信息。这些措施应包括规定以下权力：

(a) 扣押用于存储信息的信息和通信技术装置或通过其他手段取得该装置；

(b) 以电子和数字形式制作和保留该信息的副本；

(c) 维护相关已存储信息的完整性；

(d) 从该信息和通信技术装置中移除以电子形式存储或处理的信息。

4. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关根据其国内立法规定的程序，命令对相关信息系统运行、信息和电信网络或其部件或为保护其中所含信息而适用的措施具有专门知识的人员，在实施本条第 1 款至第 3 款所述措施方面提供必要信息和（或）协助。

5. 本条所述权力和程序的确立应符合本公约第 31 条和第 32 条的规定。

第 38 条 实时收集流量数据

1. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关：

(a) 为此目的运用技术手段收集或记录该缔约国境内与使用信息和通信技术有关的流量数据；

(b) 责成服务提供者在其自身技术能力范围内：

㈠ 为此目的运用技术手段收集或记录该缔约国境内的流量数据；或者

㈡ 配合并协助该缔约国主管机关实时收集或记录该缔约国境内与指定信息有关的流量数据。

2. 若缔约国由于其国内法律制度的长期既定原则而不能采取本条第 1 款(a)项所规定的措施，则可转而采取必要的立法和其他措施，确保在本国境内应用技术手段实时收集或记录本国境内的流量数据。

3. 各缔约国均应采取必要的立法和其他措施，责成服务提供者对行使本条规定的任何权力以及与之相关的任何信息保密。

4. 本条所述权力和程序应符合本公约第 31 条和第 32 条的规定。

第 39 条 管辖权

1. 各缔约国均应采取一切必要措施，在下列情况下，对本公约所确定的刑事犯罪和其他违法行为确立管辖权：

(a) 犯罪发生在该缔约国境内；或者

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

2. 在不违反本公约第 3 条规定的情况下，缔约国还可以在下列情况下，对任何犯罪和其他违法行为确立管辖权：

(a) 犯罪系针对该缔约国国民、在其境内永久居住的无国籍人士、设于其境内的法人或在其境内有常驻代表的法人、该缔约国的国家或政府设施，包括其外交使团或领事馆的馆舍；或者

(b) 犯罪者为该缔约国国民或在该国境内有惯常居所的无国籍人；或者

(c) 犯罪系针对该缔约国；或者

(d) 犯罪虽全部或部分在该缔约国境外实施，但犯罪在该缔约国境内的影响构成了犯罪或导致犯罪的实施。

3. 为本公约第 47 条之目的，各缔约国均应采取一切必要措施，在被指控犯罪人位于该缔约国境内且该国仅以此人是其本国国民或其已向此人授予难民地位为由而引渡此人时，对本公约所确定的犯罪确立管辖权。

4. 在本条第 1 款和第 2 款规定的情况下，各缔约国，若其境内有被指控犯罪人而不予引渡，无论犯罪是否发生在其境内，毫无例外，均应不加拖延地将案件提交本国主管机关，以便依照本国法律进行法律起诉。

5. 若根据本条第 1 款或第 2 款行使管辖权的缔约国被告知或以其他途径获悉，任何其他缔约国正在对同一行为进行调查、起诉或审判程序，这些缔约国的主管机关应酌情互相磋商，以便协调行动。

6. 在不影响一般国际法的情况下，本公约不排除缔约国行使其依据本国法律确立的任何刑事或行政管辖权。

第三章 预防和打击网络空间犯罪和其他违法行为的措施

[……]

第 45 条 保护证人的措施

各缔约国均应考虑采取必要的立法措施，为下列人员提供有效保护：

(a) 出于善意，基于合理理由，提供与本公约第 6 条至第 28 条所述违法行为有关的信息的人员，或以其他方式配合调查或司法机关工作的人员；

(b) 就本公约第 6 条至第 28 条所述违法行为作证的证人以及被害人；

(c) 在适当情况下，本条(a)项和(b)项所述人员的家属。

南非

[原文：英文]
[2022 年 4 月 14 日]

第三章 程序措施和执法

第 18 条：程序规定

1. 各缔约国均应采取必要的立法和其他措施，确立本条规定的权力和程序，以便进行具体的刑事调查或诉讼。

2. 除第 32 条另有具体规定外，各缔约国均应将本条第 1 款所述的权力和程序适用于：

(a) 依照本公约第[…]条至第[…]条确立的涉及使用信息和通信技术的刑事犯罪；

(b) 借助信息和通信技术实施的其他刑事犯罪；

(c) 收集涉及使用信息和通信技术的刑事犯罪的电子形式的证据。

3. 各缔约国均可保留权利，只对保留中列明的涉及使用信息和通信技术的犯罪或犯罪类别适用第 31 条所述措施，但此等犯罪或犯罪类别的范围不得比该缔约国适用第 32 条所述措施处理的犯罪范围更有限。各缔约国均应考虑限制此类保留，以便第 31 条所述措施能够得到最广泛的适用。

4. 若缔约国由于受到本公约通过时其有效立法所限，不能对使用服务提供者的信息和通信技术传输的信息适用第 31 条和第 32 条所述措施，而该系统：

(a) 正在为一个封闭用户群的利益运行，

(b) 不使用公共通信网络，也不与其他任何公共或私人信息和通信技术连接，则该缔约国可保留不对此类信息适用上述措施的权利。各缔约国均应考虑限制此类保留，以便第 31 条和第 32 条所述的措施能够得到最广泛的适用。

第 19 条：条件和保障措施

1. 各缔约国均应确保本条所规定的权力和程序的确立、实施和适用符合其国内法律规定的条件和保障，其中应规定充分保护人权和自由，包括因缔约国根据协议、条约和适用的国际人权文书承担的义务而产生的权利和基本自由，并应纳入符合缔约国主权的相称性原则。

2. 鉴于有关程序或权力的性质，此类条件和保障除其他外还应酌情包括司法监督或其他独立监督、适用的正当理由以及此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。

第 20 条：快速保全已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施，使本国主管机关能够命令或通过类似手段实现快速保全以信息和通信技术存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或被修改的情况下。

2. 若缔约国实施上述第 1 款，命令个人保全其拥有或控制的指定已存储计算机数据，则该缔约国应采取必要的立法和其他措施，责成该人在必要长的时间内保全并维护这些计算机数据的完整性，最多不超过七天，以便主管机关寻求予以披露。缔约国可以规定，此种命令嗣后可以延期。

3. 各缔约国均应采取必要的立法和其他措施，责成保管人或其他保全这些计算机数据的人在其国内法律规定的期间对执行此类程序事宜保密。

4. 本条所述权力和程序应受第 27 条和第 28 条的约束。

第 21 条：搜查和扣押已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关搜查或通过类似手段访问：

(a) 信息和通信技术、计算机系统或其一部分和存储在其中的计算机数据；

(b) 本国境内可能存储有计算机数据的计算机数据存储介质。

2. 各缔约国均应采取必要的立法和其他措施，确保若本国主管机关根据第 1 款(a)项的规定搜查或通过类似手段访问任何信息和通信技术或构成这种技术的部件、特定的计算机系统或其一部分，并有理由认为所查找的数据存储于本国境内其他信息和通信技术或构成这种技术的部件、计算机系统或其一部分，且从初始系统可合法访问或取用此类数据，则其主管机关应能够迅速搜查或通过类似手段访问该另一系统。

3. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关酌情在外国/另一缔约国的获授权官员的协助下或在场情况下，扣押或通过类似手段取得依照第 1 款或第 2 款规定所访问的计算机数据。这些措施应包括规定以下权力：

(a) 扣押或通过类似方式取得信息和通信技术或构成这种技术的部件、计算机系统或其一部分或计算机数据存储介质；

(b) 制作和保留这些计算机数据的副本；

(c) 维护相关已存储计算机数据的完整性；

(d) 使被访问计算机系统或信息和通信技术中的计算机数据无法访问或移除。

4. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关命令了解信息和通信技术运作或构成这种技术的部件、计算机系统或为保护其中所含计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够实施第 1 款和第 2 款所述的措施。

5. 本条所述权力和程序应受第 27 条和第 28 条的约束。

第 22 条：实时收集流量数据

1. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关：

(a) 应用技术手段在缔约国本国境内实时收集或记录数据；

(b) 迫使服务提供者在自身现有技术能力范围内：

㈠ 应用技术手段在缔约国本国境内实时收集或记录数据；

㈡ 配合并协助主管机关实时收集或记录本国境内借助信息和通信技术或计算机系统传输的与指定信息有关的流量数据。

第 23 条：拦截内容数据

1. 各缔约国均应就本国法律将确定的一系列严重犯罪采取必要的立法和其他措施，授权本国主管机关：

(a) 应用技术手段在本国境内实时收集或记录数据；

(b) 迫使服务提供者在自身现有技术能力范围内：

㈠ 应用技术手段在本国境内实时收集或记录数据；或者

㈡ 配合并协助主管机关实时收集或记录本国境内借助信息和通信技术或计算机系统传输的与指定信息有关的内容数据。

2. 若缔约国由于其国内法律制度既定的原则而不能采取第 1 款(a)项所述的措施，则可转而采取必要的立法和其他措施，确保应用技术手段实时收集或记录其境内与指定信息有关的内容数据。

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

4. 本条所述权力和程序应受第 27 条和第 28 条的约束。

第 24 条：冻结、扣押和没收

1. 尽管有本条规定，但不得对本条作损害善意第三方权利的解释，且本条任何规定均不得影响其所述各项措施应当依照并遵循缔约国本国法律规定加以确定和实施的原则。

2. 不得对本条规定作损害善意第三方权利的解释。

3. 本条任何规定均不得影响其所述各项措施应当依照并遵循缔约国本国法律规定加以确定和实施的原则。

4. 各缔约国均应在本国法律制度的范围内尽最大可能采取必要措施，以便能够没收：

(a) 本公约所立使用信息和通信技术造成的犯罪产生的犯罪所得或价值与此类所得和受影响缔约国的利益相当的财产；

(b) 用于或拟用于本公约所立犯罪的财产、设备或其他工具，包括信息和通信技术的使用。

4. 各缔约国均应采取必要措施，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。

5. 各缔约国均应根据其国内法律采取必要的立法和其他措施，规定主管机关对本条第 1 款和第 2 款所涵盖的冻结、扣押或没收财产的管理。

6. 如果此类犯罪所得已经部分或全部转变或转化为其他财产，则应视此类财产为犯罪所得的替代财产，适用本条所述措施。

7. 如果此类犯罪所得已与从合法来源获得的财产相混合，则应在不影响冻结权或扣押权的情况下没收此类财产，没收价值可达混合于其中的犯罪所得的估计价值。

8. 对于来自此类犯罪所得、来自此类犯罪所得转变或转化而成的财产或已与此类犯罪所得相混合的财产的收入或其他利益，也应适用本条所述的措施，其方式和程度与处置犯罪所得相同。

9. 为本公约本条和 [关于国际合作的] 第[…]条之目的，各缔约国均应授权其法院或其他主管机关命令提供或扣押银行、财务或商务记录。缔约国不应以银行保密为理由拒绝根据本款规定采取行动。

10. 缔约国可以考虑要求由犯罪人证明此类涉嫌犯罪所得或其他应予没收的财产的合法来源，但此种要求应符合其国内法律的基本原则和司法及其他程序的性质。

第 25 条：没收的犯罪所得或财产的处置

1. 缔约国依据本公约第 33 条第 3 款没收的犯罪所得或财产应由该缔约国根据其国内法律和行政程序予以处置。

2. 根据本公约第 39 条的规定应另一缔约国请求采取行动时，缔约国应在本国法律许可的范围内，根据请求，优先考虑将没收的犯罪所得或财产交还请求缔约国，以便其对犯罪被害人进行赔偿，或者将这类犯罪所得或财产归还合法所有人。

3. 一缔约国根据本公约第 41 条规定应另一缔约国请求采取行动时，可特别考虑就下述事项缔结协定或安排：

(a) 将这类犯罪所得或财产的价款，或变卖这类犯罪所得或财产所获款项，或这类款项的一部分捐给根据本公约第[…]条所指定的账户和专门从事打击有组织犯罪工作的政府间机构；

(b) 根据其国内法律或行政程序，经常地或逐案地与其他缔约国分享这类犯罪所得或财产或变卖这类犯罪所得或财产所获的款项。

第 26 条：犯罪记录

各缔约国均可采取必要的立法或其他措施，按其认为适宜的条件并为其认为适宜的目的，考虑到另一个国家以前对被指控犯罪人作出的任何有罪判决，以便在涉及本公约所立使用信息和通信技术造成的犯罪的刑事诉讼中加以利用。

第 27 条：加强与执法机关合作的措施

1. 各缔约国均应采取适当措施，鼓励参与或曾参与有组织犯罪集团的人员：

(a) 为主管机关的侦查和取证提供有用信息，例如：

㈠ 有组织犯罪集团的身份、性质、组成情况、结构、所在地或活动；

㈡ 与其他有组织犯罪集团之间的联系，包括国际联系；

㈢ 有组织犯罪集团已实施或可能实施的犯罪；

(b) 为主管机关提供可能有助于剥夺有组织犯罪集团的资源或犯罪所得的切实而具体的帮助。

2. 对于在本公约所涵盖的犯罪的侦查或起诉中真诚提供实质性配合的被指控者，各缔约国均应考虑规定在适当情况下减轻其处罚的可能性。

3. 对于在本公约所涵盖的涉及使用信息和通信技术的犯罪的侦查或起诉中真诚予以实质性配合者，各缔约国均应考虑根据其本国法律基本原则规定免予起诉的可能性。

4. 应按本公约第 34 条的规定保护此类人员。

5. 如果本条第 1 款所述的人员身在一缔约国，能真诚给予另一缔约国主管机关以实质性配合，则有关缔约国可考虑根据其本国法律订立关于由对方缔约国提供本条第 2 款和第 3 款所列待遇的协定或安排。

第 28 条：执法合作

1. 缔约国应在符合本国法律和行政管理制度的情况下相互密切合作，以加强执法行动的效力，更好地打击本公约所涵盖的涉及使用信息和通信技术的犯罪。各缔约国尤其应采取有效措施，以便：

(a) 加强并在必要时建立各国主管机关、机构和互联网服务提供者之间的联系渠道，以促进安全、迅速地交换本公约所涵盖涉及使用信息和通信技术的犯罪的各个方面的情报，有关缔约国认为适当时还可包括与其他犯罪活动的联系的有关情报；

(b) 同其他缔约国合作，就以下与本公约所涵盖涉及使用信息和通信技术的犯罪有关的事项进行调查：

㈠ 涉嫌这类犯罪的人的身份、行踪和活动，或其他有关人员的所在地点；

㈡ 来自这些犯罪的犯罪所得或财产的去向；

㈢ 用于或企图用于实施这类犯罪的财产、设备或其他工具的去向；

(c) 在适当情况下提供必要数目或数量的物品以供分析或调查之用；

(d) 促进各缔约国主管机关、机构和互联网服务提供者之间的有效协调，并加强人员和其他专家的交流，包括根据有关缔约国之间的双边协定或安排行事；

(e) 与其他缔约国交换关于有组织犯罪集团采用的具体手段和方法的资料，视情况包括关于线路和交通工具，利用假身份、经变造或伪造的证件或其他借助信息和通信技术掩盖其活动的手段的资料；

(f) 交换情报并协调为尽早查明本公约所涵盖涉及使用信息和通信技术的犯罪而酌情采取的行政和其他措施。

2. 为实施本公约，缔约国应考虑订立关于其执法机构间直接合作的双边或多边协定或安排，并在已有这类协定或安排的情况下考虑对其进行修正。如果有关缔约国之间尚未订立这类协定或安排，缔约国可考虑以本公约为基础，进行针对本公约所涵盖的任何犯罪的相互执法合作。缔约国应在适当情况下充分利用各种协定或安排，包括国际或区域组织，以加强缔约国执法机构之间的合作。

3. 缔约国应努力在力所能及的范围内开展合作，以便应对借助信息和通信技术实施的跨国有组织犯罪。

第 29 条：联合调查

缔约国应考虑缔结双边或多边协定或安排，以便有关主管机关可就一国或多国刑事侦查、起诉或审判程序所涉事由建立联合调查机构。如无这类协定或安排，则可在个案基础上商定进行这类联合调查。有关缔约国应确保拟进行这类调查的所在缔约国的主权受到充分尊重。

第 30 条：特殊侦查手段

1. 为了有效打击或制止为犯罪目的使用信息和通信技术行为，各缔约国均应在其本国法律制度基本原则许可的情况下，根据本国法律所规定的条件，在其力所能及的范围内采取必要的措施，允许在其境内使用特殊侦查手段，如电子或其他形式的监视和秘密行动，并允许法院采纳由此产生的证据，但不得威胁各缔约国的网络安全和损害其情报保密性。

2. 为侦查本公约所涵盖涉及使用信息和通信技术的犯罪，鼓励缔约国在必要时为在国际一级合作时使用这类特殊侦查手段而缔结适当的双边或多边协定或安排。此类协定或安排的缔结和实施应充分遵循各国主权平等原则，尊重基本人权和自由，执行时还应严格遵守这类协定或安排的条件。

3. 在无本条第 2 款所述协定或安排的情况下，关于在国际一级使用这种特殊侦查手段的决定，应在个案基础上作出，必要时还可考虑到有关缔约国就行使管辖权所达成的财务安排或谅解。

第 31 条：资产的返还和处分

1. 缔约国依照本公约第 33 条或第 34 条没收的财产，应当由该缔约国根据本公约的规定和本国法律予以处分，包括依照本条第 3 款返还其原合法所有人。

2. 各缔约国均应根据本国法律的基本原则，采取必要的立法和其他措施，使本国主管机关应另一缔约国请求采取行动时，能够在考虑到善意第三方权利的情况下，根据本公约返还所没收的财产。

3. 依照本条第 1 款和第 2 款：

(a) 对本公约所述的制止使用信息和通信技术实施犯罪的行为，被请求缔约国应当在依照第[…]条实行没收后，基于请求缔约国的生效判决，将所没收财产返还请求缔约国，被请求缔约国也可以放弃对生效判决的要求；

(b) 对于本公约所涵盖涉及使用信息和通信技术的其他任何犯罪的所得，被请求缔约国应当在依照本公约第[…]条实行没收后，基于请求缔约国的生效判决，在请求缔约国向被请求缔约国合理证明其原对没收的财产拥有所有权时，或者当被请求缔约国承认请求缔约国受到的损害是返还没收财产的依据时，将没收的财产返还请求缔约国，被请求缔约国也可以放弃对生效判决的要求；

(c) 在其他所有情况下，被请求缔约国优先考虑将没收的财产返还请求缔约国、返还其原合法所有人或者赔偿犯罪被害人。

4. 在适当情况下，除非缔约国另有决定，被请求缔约国可以在依照本条规定返还或者处分没收的财产之前，扣除为此进行侦查、起诉或者审判程序而发生的合理费用。

5. 在适当的情况下，缔约国根据本国立法，还可以特别考虑就所没收财产的最后处分逐案订立协定或者可以共同接受的安排。

瑞士

[原文：英文]
[2022 年 4 月 8 日]

2.3 有关程序措施和执法的规定

第 1 节

共同条款

程序规定的范围

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

2. 各缔约国均应将本条第 1 款所述的权力和程序适用于：

(a) 依照本公约刑事定罪规定确立的刑事犯罪；

(b) 借助计算机系统实施的其他刑事犯罪；

(c) 收集刑事犯罪的电子形式的证据。

3. (a) 各缔约国均可保留权利，只对保留中列明的犯罪或犯罪类别适用实时收集流量数据的措施，但此等犯罪或犯罪类别的范围不得比该缔约国适用拦截内容数据的措施处理的犯罪范围更有限。各缔约国均应考虑限制此类保留，以便实时收集流量数据措施能够得到最广泛的适用。

(b) 若缔约国由于受到本公约通过时其有效立法所限，不能对服务提供者计算机系统内传输的信息适用实时收集流量数据和拦截内容数据措施，而该系统：

㈠ 正在为一个封闭用户群的利益运行；

㈡ 不使用公共通信网络，也不与其他公共或私人计算机系统连接，

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

条件和保障措施

1. 各缔约国均应确保本节规定的权力和程序的确立、实施和适用符合其国内法所规定的条件和保障，其中应规定充分保护人权和自由，包括缔约国依照《公民及政治权利国际公约》和其他适用国际和区域人权文书承担的义务而产生的权利，并应纳入相称性原则。

2. 鉴于有关程序或权力的性质，此类条件和保障除其他外还应酌情包括司法监督或其他独立监督、适用的正当理由以及此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节规定的权力和程序对第三方权利、责任和合法利益的影响。

快速保全已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施，使本国主管机关能够命令或通过类似手段实现快速保全以计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据极易丢失或被修改的情况下。

2. 若缔约国实施上述第 1 款，命令个人保全其拥有或控制的指定已存储计算机数据，则该缔约国应采取必要的立法和其他措施，责成该人在必要长的期限内保全并维护这些计算机数据的完整性，最多不超过 90 天，以便主管机关寻求予以披露。缔约国可以规定，此种命令嗣后可以延期。

3. 各缔约国均应采取必要立法和其他措施，责成保管人或其他保全这些计算机数据的人在缔约国本国法律规定的期间对执行此类程序事宜保密。

4. 本条所述权力和程序应符合本公约有关程序规定的范围以及条件和保障措施的规定。

提交令

1. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关：

(a) 命令本国境内人员提交其拥有或控制的存储于计算机系统或计算机数据存储介质中的指定计算机数据；

(b) 命令在缔约国本国境内提供服务的服务提供者提交其拥有或控制的与服务有关的用户信息。

2. 本条所述权力和程序应符合本公约有关程序规定的范围以及条件和保障措施的规定。

3. 就本条目的而言，“用户信息”一词系指服务提供者掌握的以计算机数据形式或任何其他形式存储的除流量数据或内容数据之外与其服务用户有关的任何信息，基于这些信息有可能确定：

(a) 使用的通信服务类型，对其采用的技术规定和服务期；

(b) 根据服务协议或安排可获取的用户身份、邮政地址或地理位址、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可获取的关于通信设备安装地点的任何其他信息。

搜查和扣押已存储的计算机数据

1. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关搜查或通过类似手段访问：

(a) 计算机系统或其一部分以及其中存储的计算机数据；

(b) 其本国境内可能存储有计算机数据的计算机数据存储介质。

2. 各缔约国均应采取必要的立法和其他措施，确保若本国主管机关根据第 1 款(a)项的规定搜查或通过类似手段访问特定的计算机系统或其一部分，并有理由相信所查找的数据存储于本国境内另一计算机系统或其一部分内，且从初始系统可合法访问或取用这些数据，则该主管机关应能够迅速搜查或通过类似手段访问该另一系统。

3. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关扣押或通过类似手段取得依照第 1 款或第 2 款规定所访问的信息。这些措施应包括规定以下权力：

(a) 扣押或通过类似手段取得计算机系统或其一部分或计算机数据存储介质；

(b) 制作和保留该计算机数据的副本；

(c) 维护相关已存储信息的完整性；

(d) 使被访问计算机系统中的计算机数据无法访问或移除。

4. 各缔约国均应采取必要的立法和其他措施，授权本国主管机关命令了解计算机系统的运作或为保护其中所含计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够实施第 1 款和第 2 款所述的措施。

5. 本条所述权力和程序应符合本公约有关程序规定的范围以及条件和保障措施的规定。

第 2 节

管辖权

1. 各缔约国均应采取必要的立法和其他措施，在下列情况下，对依照本公约刑事定罪规定确立的任何犯罪确立管辖权：

(a) 犯罪发生在该缔约国境内；或者

(b) 犯罪发生在悬挂该缔约国国旗的船只上或根据该缔约国法律注册的航空器内；或者

(c) 犯罪系由其国民所实施，条件是该犯罪行为根据犯罪实施地所在国家的法律应当受到惩罚，或实施犯罪是在任何国家的领土管辖范围之外。

2. 各缔约国均可保留权利，不适用或只在特定情况或条件下适用本条第 1 款(b)项至第 1 款(d)项规定的管辖权规则或其任何部分。

3. 各缔约国均应采取必要措施，对依照本公约刑事定罪规定确立的犯罪行为确立管辖权，针对的情况是，被指控犯罪人位于本国境内，在接到引渡请求后仅以该人的国籍为由不将其引渡到另一缔约国，但该犯罪行为根据有关缔约国双方法律都应处以剥夺自由（最高刑期至少一年）或更严厉的刑罚。

4. 缔约国还可在下列情况下，对依照本公约刑事定罪规定确立的任何犯罪行为确立管辖权：

(a) 犯罪系针对该缔约国国民；

(b) 犯罪系针对该缔约国。

5. 本公约不排除缔约国依照其本国法律行使的任何刑事管辖权。

6. 当一个以上缔约国对依照本公约确立的受指控犯罪主张管辖权时，有关缔约国应适当协商，以确定最适当的起诉管辖权。

大不列颠及北爱尔兰联合王国

[原文：英文]
[2022 年 4 月 12 日]

第 章 程序措施和执法

第 16 条
条件和保障措施

1. 各缔约国应确保本节所规定权力和程序的确立、执行和适用遵守其国内法规定的条件和保障措施，其中应规定充分保护人权和自由，包括根据其依照《公民及政治权利国际公约》和其他适用的国际人权法承担的义务而产生的权利，并应纳入相称性原则。

2. 鉴于有关程序或权力的性质，此类条件和保障措施除其他外还应酌情包括司法或其他独立监督、适用的正当理由以及此类权力或程序范围和期限的限制。

3. 在符合公共利益，特别是健全司法的范围内，各缔约国均应考虑本节规定的权力和程序对第三方的权利、责任和合法利益的影响。

第 17 条
程序规定的范围，包括对所有犯罪更广泛地使用程序法

1. 各缔约国应采取必要的立法和其他措施，确立本节规定的权力和程序，以便进行具体的刑事侦查或诉讼。

2. 除非另有明确规定，否则各缔约国应将本条第 1 款所述权力和程序适用于：

(a) 根据本公约定义的罪行确定的刑事犯罪；

(b) 利用计算机系统实施的其他刑事犯罪；

(c) 收集刑事犯罪的电子形式的证据。

第 18 条
加速保全

1. 各缔约国应采取必要的立法和其他措施，使其主管机关能够下令或以类似方式实现快速保全通过计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或被修改的情况下。

2. 如果缔约国实施上文第 1 款，命令某人保全其拥有或控制的指定存储计算机数据，该缔约方应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护该计算机数据的完整性，最长不超过 90 天，以便主管机关能够寻求予以披露。缔约国可以规定，此种命令嗣后可延期。

3. 各缔约国应采取必要的立法和其他措施，责成保管人或其他负责保全计算机数据的人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有人权保障措施。

第 19 条
提交令

1. 各缔约国应采取必要的立法和其他措施，授权其主管机关命令：

(a) 在本国领土内的某人提交由该人拥有或控制的指定计算机数据，不论这些数据是存储在计算机系统内还是存储在计算机数据存储介质中；

(b) 在缔约国境内提供服务的服务提供者提交其拥有或控制的与此类服务相关的用户信息。

(c) 本条所述权力和程序应有人权保障措施。

2. 在本条中，“用户信息”一词系指服务提供者掌握的以计算机数据形式或任何其他形式存储的除流量数据或内容数据之外与其服务用户有关的信息，通过这些信息可以确定：

(a) 所用通信服务类型、为此采用的技术规定和服务期限；

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

(c) 根据服务协议或安排可提供的有关通信设备安装地点的任何其他信息。

第 20 条
搜查和扣押已存储的计算机数据

1. 各缔约国应采取必要的立法和其他措施，授权其主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及存储在其中的计算机数据；

(b) 在本国领土内可能存储计算机数据的计算机数据存储介质。

2. 各缔约国应采取必要的立法和其他措施，确保若其主管机关根据第 1 款(a)项搜查或以类似方式访问某一特定计算机系统或其一部分，并有理由认为所寻找数据存储在其领土内的另一计算机系统或其一部分中，且可从初始系统合法访问或取用此类数据，则其主管机关应能迅速将搜查或类似访问扩大到该另一系统。

3. 各缔约国应采取必要的立法和其他措施，授权其主管机关扣押或以类似方式获取根据第 1 款或第 2 款访问的计算机数据。这些措施应包括以下权力：

(a) 扣押或以类似方式获取计算机系统或其一部分或计算机数据存储介质；

(b) 制作并保留这些计算机数据的副本；

(c) 维护相关所存储计算机数据的完整性；

(d) 使被访问的计算机系统中的那些计算机数据不可访问或移除。

4. 各缔约国应采取必要的立法和其他措施，授权其主管机关命令任何了解计算机系统运行情况或为保护系统中的计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取第 1 款和第 2 款所述的措施。

5. 本条所述权力和程序应有人权保障措施。

坦桑尼亚联合共和国

[原文：英文]
[2022 年 4 月 8 日]

5. 程序措施

关于网络犯罪的法律确定了信息和通信技术用户可接受的行为标准，确立了对网络犯罪的社会法律制裁，总体上保护信息和通信技术用户，减轻和（或）防止损害人、数据、系统、服务和基础设施。坦桑尼亚联合共和国建议该公约在程序措施一节中包括以下方面。

加快保全和披露电子数据

该公约应规定会员国在其国内立法中载入必要的措施，使其主管机关能够命令或以类似方式实现快速保全通过计算机系统存储的指定电子数据，包括流量数据，特别是在有理由认为电子数据特别容易丢失或被修改的情况下。

如果通过命令某人保全由其拥有或控制的指定存储电子数据，缔约国应采取必要的立法和其他措施，责成该人在必要长的期限内保全和维护电子数据的完整性，以便主管机关能够寻求披露这些数据。缔约国可以规定这种命令嗣后可以延期。

公约应规定会员国采取必要的立法和其他措施，责成保全计算机数据的保管人或其他人在其国内法规定的时间内对实施此类程序事宜保密。

提交令

公约中应规定必要的立法和其他措施，授权主管机关命令其境内的个人提交其拥有或控制的、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。

搜查和扣押已存储的计算机数据

公约必须规定会员国有义务在其立法和其他必要措施中作出规定，授权其主管机关搜查、访问和扣押其境内的可能存储了计算机数据的计算机系统或其一部分、其中存储的计算机数据。

保护举报人和证人

公约应规定缔约国有义务根据案情需要保护网络犯罪的举报人、证人和受害人。

还建议公约应指示会员国在其力所能及的范围内采取适当措施，根据本国法律，为刑事诉讼中就公约所涵盖犯罪提供信息或证词的举报人和证人，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。这些措施不应损害被告的权利，包括正当程序权。

6. 执法

对网络犯罪和相关犯罪的适当管理需要预防、侦查和打击不同过程的参与。因此，这些授权给执法机构的程序需要得到承认。因此，坦桑尼亚联合共和国认为，公约应涵盖与执法有关的以下方面。

培训、技术援助和专门知识交流

为了有效预防和打击将信息和通信技术用于犯罪目的，必须向发展中国家提供技术援助并加强信息交流。技术援助和专门知识交流应侧重于以下方面：

(a) 侦查、预防和打击公约所涵盖的犯罪；

(b) 参与公约所涵盖罪行的嫌疑人使用的技术和适当的反措施；

(c) 监测违禁品的流动；

(d) 侦查和监测犯罪所得、财产、设备或工具以及用于转移、隐藏或掩饰这类所得和工具的方法，以及用于打击网络犯罪的方法；

(e) 收集证据；

(f) 现代执法设备和技术，包括使用新软件和卧底行动；

(g) 打击利用计算机系统、电信网络或其他形式的现代技术实施的网络犯罪的方法；

(h) 规划和实施旨在分享网络空间保护专门知识的研究和培训方案。

联合调查

网络犯罪本质上是无国界的，可能涉及一个以上的国家。公约应规定缔约国有义务就一国或多国调查、起诉或审判程序的主题事项作出安排。有关主管机关可以成立联合调查机构。敦促有关缔约国确保在某缔约国领土上进行此类调查时充分尊重该缔约国的主权。

财政支持

公约下应有一项规定，规定发达国家和联合国机构有义务向发展中国家提供财政支持，以便实施侦查、预防和打击网络犯罪的战略。

美利坚合众国

[原文：英文]
[2022 年 4 月 8 日]

程序措施和执法

程序规定

程序规定的范围

1. 各缔约国应采取必要的立法和其他措施，确立本节规定的权力和程序，以便进行具体的刑事侦查或诉讼。

2. 除非关于拦截内容数据的条款另有明确规定，各缔约国应将本条第 1 款所述权力和程序适用于：

(a) 根据本公约定罪一章确立的刑事犯罪；

(b) 借助计算机系统实施的其他刑事犯罪；

(c) 收集刑事犯罪的电子形式的证据。

加速保全已存储的计算机数据

1. 各缔约国应采取必要的立法和其他措施，使其主管机关能够命令或以类似方式实现快速保全通过计算机系统存储的指定计算机数据，包括流量数据，特别是在有理由认为计算机数据特别容易丢失或被修改的情况下。

2. 如果缔约国实施上文第 1 款，命令某人保全其拥有或控制的指定存储计算机数据，该缔约国应采取必要的立法和其他措施，责成该人在必要的一段时间内保全和维护该计算机数据的完整性，最长不超过 90 天，以便主管机关能够寻求予以披露。缔约国可以规定，此种命令嗣后可延期。

3. 各缔约国应采取必要的立法和其他措施，责成保管人或其他负责保全计算机数据的人在其国内法规定的期限内对采取此类程序事宜保密。

提交令

1. 各缔约国应采取必要的立法和其他措施，授权其主管机关命令其境内的人提交其掌握或控制的、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；

搜查和扣押已存储的计算机数据

1. 各缔约国应采取必要的立法和其他措施，授权其主管机关搜查或以类似方式访问：

(a) 计算机系统或其一部分以及其中存储的计算机数据；

(b) 其领土内可以存储计算机数据的计算机数据存储介质。

2. 各缔约国应采取必要的立法和其他措施，确保若其主管机关根据第 1 款(a)项搜查或以类似方式访问某一特定计算机系统或其一部分，并有理由相信所搜查的数据存储在其领土内的另一计算机系统或其一部分中，且可从初始系统合法访问或取用此类数据，则其主管机关应能迅速将搜查或类似访问扩大到该另一系统。

3. 各缔约国应采取必要的立法和其他措施，授权其主管机关扣押或以类似方式获取根据第 1 款或第 2 款访问的计算机数据。这些措施应包括以下权力：

(a) 扣押或以类似方式获取计算机系统或其部分或计算机数据存储介质；

(b) 制作并保留这些计算机数据的副本；

(c) 维护相关所存储计算机数据的完整性；

(d) 使被访问的计算机系统中的那些计算机数据不可访问或移除。

4. 各缔约国应采取必要的立法和其他措施，授权其主管机关命令任何了解计算机系统运行或为保护系统中的计算机数据而适用的措施的人，在合理的情况下，提供必要信息，以便能够采取第 1 款和第 2 款所述的措施。

实时收集流量数据

1. 各缔约国均应采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国领土上应用技术手段收集或记录；

(b) 迫使服务提供者在其现有技术能力范围内：

㈠ 在该缔约国领土上应用技术手段收集或记录；或者

㈡ 配合并协助主管机关实时收集或记录与其境内借助计算机系统传输的指定通信相关的流量数据。

2. 如果一个缔约国由于其国内法律制度的既定原则而不能采取第 1 款(a)项所述的措施，它可以采取必要的立法和其他措施，确保在其领土上应用技术手段，实时收集或记录与在其领土上传输的指定通信有关的流量数据。

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

拦截内容数据

1. 各缔约国应对将由本国法律确定的一系列严重犯罪采取必要的立法和其他措施，授权其主管机关：

(a) 在该缔约国领土上应用技术手段收集或记录；

(b) 迫使服务提供者在其现有技术能力范围内：

㈠ 在该缔约国领土上应用技术手段收集或记录；或者

㈡ 配合并协助主管机关实时收集或记录其境内借助计算机系统传输的指定通信的内容数据。

2. 如果一个缔约国由于其国内法律制度的既定原则而不能采取第 1 款(a)项所述的措施，它可以采取必要的立法和其他措施，确保在其领土上应用技术手段，实时收集或记录与在其领土上传输的指定通信有关的内容数据。

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

管辖权[17]

1. 各缔约国应采取必要措施，在下列情况下，对依本公约确定的犯罪确立管辖权：

(a) 犯罪发生在该缔约国境内；或者

(b) 犯罪发生在犯罪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. 在不违反本公约主权条款的情况下，缔约国在下列情况下还可对任何此种犯罪确立其管辖权：

(a) 犯罪系针对该缔约国国民；或者

(b) 犯罪者为该缔约国国民或在其境内有惯常居所的无国籍人；或者

(c) 该犯罪系根据本公约[洗钱条款]条款确立的犯罪之一，在其领土以外实施，目的是在其领土内实施根据本公约[洗钱条款]条款确立的犯罪；或者

(d) 犯罪系针对该缔约国。

3. 为了本公约引渡条款的目的，各缔约国应采取必要措施，在被指控犯罪人在其领域内，而其仅因该人系其本国国民而不予引渡时，确立其对根据本公约确定的犯罪的管辖权。

4. 各缔约国还可采取必要措施，在被指控犯罪人在其领域内而其不引渡该人时确立其对根据本公约确定的犯罪的管辖权。

[17] 《联合国反腐败公约》第四十二条和《联合国打击跨国有组织犯罪公约》第 十五 条。

5. 如果根据本条第 1 款或第 2 款行使其管辖权的缔约国被告知或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、起诉或审判程序，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依据本国法律确立的任何刑事管辖权。

没收和扣押[18]

1. 缔约国应在本国法律制度的范围内尽最大可能采取必要措施，以便能够没收：

(a) 本公约所涵盖犯罪产生的犯罪所得或价值与其相当的财产；

(b) 用于或拟用于本公约所涵盖的犯罪的财产、设备或其他工具。

2. 缔约国应采取必要措施，以能够辨认、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. 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，则应将此类财产视为犯罪所得的替代财产，适用本条所述措施。

4. 如果犯罪所得已与从合法来源获得的财产相混合，则应在不影响冻结权或扣押权的情况下没收这类财产，没收价值可达混合于其中的犯罪所得的估计价值。

5. 对于来自犯罪所得、来自由犯罪所得转变或转化而成的财产或已与犯罪所得相混合的财产的收入或其他利益，也应适用本条所述措施，其方式和程度与处置犯罪所得相同。

6. 为本公约本条和[没收事宜的国际合作]条款的目的，各缔约国均应授权其法院或其他主管机关提供或扣押银行、财务或商业记录。缔约国不得以银行保密为由拒绝按照本款规定采取行动。

7. 缔约国可考虑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的可能性，但此种要求应符合其本国法律原则和司法及其他程序的性质。

8. 不得对本条规定作损害善意第三方权利的解释。

9. 本条任何规定均不得影响本条所述措施应根据且遵守缔约国本国法律规定予以确定和实施的原则。

没收的犯罪所得或财产的处置[19]

1. 缔约国依照本公约关于没收和扣押的条款和[关于没收事宜的国际合作的任何条款]没收的犯罪所得或财产应由该缔约国根据其国内法和行政程序予以处置。

2. 根据本公约条款[关于没收事宜的国际合作的任何条款]应另一缔约国的请求采取行动时，缔约国应在本国法律允许的范围内，根据请求，优先考虑将没收的犯

[18] 《有组织犯罪公约》，第十二条。

[19] 《有组织犯罪公约》，第十四条。

罪所得或财产交还请求缔约国，以便其对犯罪被害人进行赔偿，或将这类犯罪所得或财产归还其合法所有人。

3. 根据本公约关于没收和扣押以及[没收事宜的任何国际合作]的条款应另一缔约国的请求采取行动时，缔约国在适当考虑对被害人的赔偿之后，可特别考虑就下列事项缔结协定或安排：

(a) 将这类犯罪所得或财产的价款，或变卖这类犯罪所得或财产所得的款项，或这类款项的一部分捐给根据本公约[任何技术援助条款]指定的账户和专门打击网络犯罪的政府间机构；

(b) 根据其国内法或行政程序，经常或逐案与其他缔约国分享这种犯罪所得或财产，或变卖这种犯罪所得或财产所得款项。

建立犯罪记录[20]

各缔约国均可采取必要的立法或其他措施，按其认为适宜的条件并为其认为适宜的目的，考虑另一国以前对被指控犯罪人所作的任何有罪判决，以便在涉及本公约所涵盖犯罪的刑事诉讼中使用这种信息。

保护证人[21]

1. 各缔约国均应在其力所能及的范围内采取适当的措施，为刑事诉讼中就本公约所涵盖的犯罪作证的证人并酌情为其亲属及其他与其关系密切的人提供有效的保护，使其免遭可能的报复或恐吓。

2. 在不影响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) 制定向此种人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限制披露有关其身份和下落的情况；

(b) 规定可允许证人以确保其安全的方式作证的证据规则，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 款所述人员的协定或安排。

4. 本条的规定也应适用于作为证人的被害人。

帮助和保护被害人[22]

1. 各缔约国均应在其力所能及的范围内采取适当的措施，以便向本公约所涵盖的犯罪的被害人提供帮助和保护，尤其是在其受到报复威胁或恐吓的情况下。

[20] 《有组织犯罪公约》，第二十二条。

[21] 《有组织犯罪公约》，第二十四条和《反腐败公约》，第三十二条。

[22] 《有组织犯罪公约》，第 二十五 条。

2. 各缔约国均应制定适当的程序，使本公约所涵盖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其本国法律的情况下，在对犯罪人提起的刑事诉讼的适当阶段，以不损害被告人权利的方式使被害人的意见和关切得到表达和考虑。

加强与执法机关合作的措施[23]

1. 各缔约国均应采取适当措施，鼓励参与或曾参与本公约所定犯罪的人：

(a) 为主管机关的侦查和取证提供有用信息，例如：

㈠ 参与本公约所定犯罪的人的身份、性质、组成情况、结构、所在地或活动；

㈡ 与参与本公约所定犯罪的其他人的联系，包括国际联系；

㈢ 参与本公约所定犯罪的人已经实施或可能实施的犯罪；

(b) 向主管机关提供可能有助于剥夺[参与本公约所定犯罪的人]的资源或犯罪所得的实际、具体的帮助。

2. 对于在侦查或起诉本公约所涵盖犯罪时予以实质性配合的被指控人，各缔约国均应考虑规定在适当情况下减轻处罚的可能性。

3. 对于本公约所涵盖的犯罪的侦查或起诉中予以实质性配合者，各缔约国均应考虑根据其国内法基本原则规定允许免予起诉的可能性。

4. 应按本公约关于保护证人的条款的规定为此类人员提供保护。

5. 如果本条第 1 款所述的、位于一缔约国的人员能给予另一缔约国主管机关以实质性配合，有关缔约国可考虑根据其国内法订立关于由对方缔约国提供本条第 2 款和第 3 款所列待遇的协定或安排。

委内瑞拉玻利瓦尔共和国

[原文：西班牙文]
[2022 年 4 月 13 日]

6. 程序措施和执法

关于刑事诉讼和执法，总的来说，建议这项未来的公约建立涉及以下方面的机制：

- 确定查明和分享证据以及其他调查阶段的合作机制。
- 界定确定非国家行为者责任的机制，并建立监管框架，界定这些行为者在执行国家和国际法律过程中的义务范围。
- 在刑事侦查中，确立对使用信通技术的管辖权，促进合作，并且不影响国家主权。

[23] 《有组织犯罪公约》， 第 二十六 条。

越南

[原文：英文]
[2022 年 4 月 12 日]

第三章
程序措施和执法

8. *管辖权*

1. 各会员国应采取必要措施，在下列情况下确立其对第[…]条所述罪行的管辖权：

(a) 罪行系在该国管辖的任何领土上或在该国注册的船只或航空器上实施；

(b) 被指控的犯罪人系该国国民；

(c) 当受害者系该国国民时，在该国认为适当的情况下。

2. 本公约不排除一国根据其国内法行使的任何刑事管辖权。

9. *主管机关的权力*

会员国应：

(a) 采取措施，预防、辨认、侦查、起诉实施本公约所涵盖的刑事犯罪的行为，启动相关审判程序；

(b) 以保护其他会员国主权的方式收集与本公约所涵盖犯罪有关的证据，包括数字数据。