（2024 年 8 月，第一期）

目录

一、法规速递

《网络暴力信息治理规定》

发文机关：国家互联网信息办公室、公安部、文化和旅游部、国家广播电视总局

发布时间：2024.06.12

生效时间：2024.08.01

第一章 总 则

第一条 为了治理网络暴力信息，营造良好网络生态，保障公民合法权益，维护社会公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 中华人民共和国境内的网络暴力信息治理活动，适用本规定。

第三条 网络暴力信息治理坚持源头防范、防控结合、标本兼治、协同共治的原则。

第四条 国家网信部门负责统筹协调全国网络暴力信息治理和相关监督管理工作。国务院公安、文化和旅游、广播电视等有关部门依据各自职责开展网络暴力信息的监督管理工作。

地方网信部门负责统筹协调本行政区域内网络暴力信息治理和相关监督管理工作。地方公安、文化和旅游、广播电视等有关部门依据各自职责开展本行政区域内网络暴力信息的监督管理工作。

第五条 鼓励网络相关行业组织加强行业自律，开展网络暴力信息治理普法宣传，督促指导网络信息服务提供者加强网络暴力信息治理并接受社会监督，为遭受网络暴力信息侵害的用户提供帮扶救助等支持。

第二章 一般规定

第六条 网络信息服务提供者和用户应当坚持社会主义核心价值观，遵守法律法规，尊重社会公德和伦理道德，促进形成积极健康、向上向善的网络文化，维护良好网络生态。

第七条 网络信息服务提供者应当履行网络信息内容管理主体责任，建立完善网络暴力信息治理机制，健全用户注册、账号管理、个人信息保护、信息发布审核、监测预警、识别处置等制度。

第八条 网络信息服务提供者为用户提供信息发布、即时通讯等服务的，应当依法对用户进行真实身份信息认证。用户不提供真实身份信息的，网络信息服务提供者不得为其提供相关服务。

网络信息服务提供者应当加强用户账号信息管理，为遭受网络暴力信息侵害的相关主体提供账号信息认证协助，防范和制止假冒、仿冒、恶意关联相关主体进行违规注册或者发布信息。

第九条 网络信息服务提供者应当制定和公开管理规则、平台公约，与用户签订服务协议，明确网络暴力信息治理相关权利义务，并依法依约履行治理责任。

第十条 任何组织和个人不得制作、复制、发布、传播涉网络暴力违法信息，应当防范和抵制制作、复制、发布、传播涉网络暴力不良信息。

任何组织和个人不得利用网络暴力事件实施蹭炒热度、推广引流等营销炒作行为，不得通过批量注册或者操纵用户账号等形式组织制作、复制、发布、传播网络暴力信息。

明知他人从事涉网络暴力信息违法犯罪活动的，任何组织和个人不得为其提供数据、技术、流量、资金等支持和协助。

第十一条 网络信息服务提供者应当定期发布网络暴力信息治理公告，并将相关工作情况列入网络信息内容生态治理工作年度报告。

第三章 预防预警

第十二条 网络信息服务提供者应当在国家网信部门和国务院有关部门指导下细化网络暴力信息分类标准规则，建立健全网络暴力信息特征库和典型案例样本库，采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络暴力信息的识别监测。

第十三条 网络信息服务提供者应当建立健全网络暴力信息预警模型，综合事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等因素，及时发现预警网络暴力信息风险。

网络信息服务提供者发现存在网络暴力信息风险的，应当及时回应社会关切，引导用户文明互动、理性表达，并对异常账号及时采取真实身份信息动态核验、弹窗提示、违规警示、限制流量等措施；发现相关信息内容浏览、搜索、评论、举报量显著增长等情形的，还应当及时向有关部门报告。

第十四条 网络信息服务提供者应当建立健全用户账号信用管理体系，将涉网络暴力信息违法违规情形记入用户信用记录，依法依约降低账号信用等级或者列入黑名单，并据以限制账号功能或者停止提供相关服务。

第四章 信息和账号处置

第十五条 网络信息服务提供者发现涉网络暴力违法信息的，或者在其服务的醒目位置、易引起用户关注的重点环节发现涉网络暴力不良信息的，应当立即停止传输，采取删除、屏蔽、断开链接等处置措施，保存有关记录，向有关部门报告。发现涉嫌违法犯罪的，应当及时向公安机关报案，并提供相关线索，依法配合开展侦查、调查和处置等工作。

第十六条 互联网新闻信息服务提供者应当坚持正确政治方向、舆论导向、价值取向，加强网络暴力信息治理的公益宣传。

互联网新闻信息服务提供者不得通过夸大事实、过度渲染、片面报道等方式采编发布、转载涉网络暴力新闻信息。对互联网新闻信息提供跟帖评论服务的，应当实行先审后发。

互联网新闻信息服务提供者采编发布、转载涉网络暴力新闻信息不真实或者不公正的，应当立即公开更正，消除影响。

第十七条 网络信息服务提供者应当加强网络视听节目、网络表演等服务内容的管理，发现含有网络暴力信息的网络视听节目、网络表演等服务的，应当及时删除信息或者停止提供相关服务；应当加强对网络直播、短视频等服务的内容审核，及时阻断含有网络暴力信息的网络直播，处置含有网络暴力信息的短视频。

第十八条 网络信息服务提供者应当加强对跟帖评论信息内容的管理，对以评论、回复、留言、弹幕、点赞等方式制作、复制、发布、传播网络暴力信息的，应当及时采取删除、屏蔽、关闭评论、停止提供相关服务等处置措施。

第十九条 网络信息服务提供者应当加强对网络论坛社区和网络群组的管理，禁止用户在版块、词条、超话、群组等环节制作、复制、发布、传播网络暴力信息，禁止以匿名投稿、隔空喊话等方式创建含有网络暴力信息的论坛社区和群组账号。

网络论坛社区、网络群组的建立者和管理者应当履行管理责任，发现用户制作、复制、发布、传播网络暴力信息的，应当依法依约采取限制发言、移出群组等管理措施。

第二十条 公众账号生产运营者应当建立健全发布推广、互动评论等全过程信息内容安全审核机制，发现账号跟帖评论等环节存在网络暴力信息的，应当及时采取举报、处置等措施。

第二十一条 对违反本规定第十条的用户，网络信息服务提供者应当依法依约采取警示、删除信息、限制账号功能、关闭账号等处置措施，并保存相关记录；对组织、煽动、多次发布网络暴力信息的，网络信息服务提供者还应当依法依约采取列入黑名单、禁止重新注册等处置措施。

对借网络暴力事件实施营销炒作等行为的，除前款规定外，还应当依法依约采取清理订阅关注账号、暂停营利权限等处置措施。

第二十二条 对组织、煽动制作、复制、发布、传播网络暴力信息的网络信息内容多渠道分发服务机构，网络信息服务提供者应当依法依约对该机构及其管理的账号采取警示、暂停营利权限、限制提供服务、入驻清退等处置措施。

第五章 保护机制

第二十三条 网络信息服务提供者应当建立健全网络暴力信息防护功能，提供便利用户设置屏蔽陌生用户或者特定用户、本人发布信息可见范围、禁止转载或者评论本人发布信息等网络暴力信息防护选项。

网络信息服务提供者应当完善私信规则，提供便利用户设置仅接收好友私信或者拒绝接收所有私信等网络暴力信息防护选项，鼓励提供智能屏蔽私信或者自定义私信屏蔽词等功能。

第二十四条 网络信息服务提供者发现用户面临网络暴力信息风险的，应当及时通过显著方式提示用户，告知用户可以采取的防护措施。

网络信息服务提供者发现网络暴力信息风险涉及以下情形的，还应当为用户提供网络暴力信息防护指导和保护救助服务，协助启动防护措施，并向网信、公安等有关部门报告：

（一）网络暴力信息侵害未成年人、老年人、残疾人等用户合法权益的；

（二）网络暴力信息侵犯用户个人隐私的；

（三）若不及时采取措施，可能造成用户人身、财产损害等严重后果的其他情形。

第二十五条 网络信息服务提供者发现、处置网络暴力信息的，应当及时保存信息内容、浏览评论转发数量等数据。网络信息服务提供者应当向用户提供网络暴力信息快捷取证等功能，依法依约为用户维权提供便利。

公安、网信等有关部门依法调取证据的，网络信息服务提供者应当及时提供必要的技术支持和协助。

第二十六条 网络信息服务提供者应当自觉接受社会监督，优化投诉、举报程序，在服务显著位置设置专门的网络暴力信息快捷投诉、举报入口，公布处理流程，及时受理、处理公众投诉、举报并反馈处理结果。

网络信息服务提供者应当结合投诉、举报内容以及相关证明材料及时研判。对属于网络暴力信息的投诉、举报，应当依法处理并反馈结果；对因证明材料不充分难以准确判断的，应当及时告知用户补充证明材料；对不属于网络暴力信息的投诉、举报，应当

按照其他类型投诉、举报的受理要求予以处理并反馈结果。

第二十七条 网络信息服务提供者应当优先处理涉未成年人网络暴力信息的投诉、举报。发现涉及侵害未成年人用户合法权益的网络暴力信息风险的，应当按照法律法规和本规定要求及时采取措施，提供相应保护救助服务，并向有关部门报告。

网络信息服务提供者应当设置便利未成年人及其监护人行使通知删除网络暴力信息权利的功能、渠道，接到相关通知后，应当及时采取删除、屏蔽、断开链接等必要的措施，防止信息扩散。

第六章 监督管理和法律责任

第二十八条 网信部门会同公安、文化和旅游、广播电视等有关部门依法对网络信息服务提供者的网络暴力信息治理情况进行监督检查。

网络信息服务提供者对网信部门和有关部门依法实施的监督检查应当予以配合。

第二十九条 网信部门会同公安、文化和旅游、广播电视等有关部门建立健全信息共享、会商通报、取证调证、案件督办等工作机制，协同治理网络暴力信息。

公安机关对于网信、文化和旅游、广播电视等部门移送的涉网络暴力信息违法犯罪线索，应当及时进行审查，并对符合立案条件的及时立案侦查、调查。

第三十条 违反本规定的，依照《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规的规定予以处罚。

法律、行政法规没有规定的，由网信、公安、文化和旅游、广播电视等有关部门依据职责给予警告、通报批评，责令限期改正，可以并处一万元以上十万元以下罚款；涉及危害公民生命健康安全且有严重后果的，并处十万元以上二十万元以下罚款。

对组织、煽动制作、复制、发布、传播网络暴力信息或者利用网络暴力事件实施恶意营销炒作等行为的组织和个人，应当依法从重处罚。

第三十一条 违反本规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第三十二条 本规定所称网络暴力信息，是指通过网络以文本、图像、音频、视频等形式对个人集中发布的，含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等内容的违法和不良信息。

第三十三条 依法通过网络检举、揭发他人违法犯罪，或者依法实施舆论监督的，不适用本规定。

第三十四条 本规定自 2024 年 8 月 1 日起施行。

《北京国际大数据交易所有限责任公司个人信息授权运营管理办法（试行）》

发文机构：北京国际大数据交易所

发布时间：2024.08.01

生效时间：2024.08.01

第一章 总 则

第一条 为落实《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》中“建立健全个人信息数据确权授权机制”和中共北京市委、北京市人民政府印发的《关于更好发挥数据要素作用进一步加快发展数字经济的实施意见》中“推进建立个人数据分类分级确权授权机制”相关要求，进一步巩固北京数据基础制度先行区工作成果，规范个人信息授权运营管理，确保个人信息主体对自身数据使用情况享有的知情权、决定权和收益权，推动数据的合法、合理利用及价值实现，根据《中华人民共和国个人信息保护法》（以下简称“《个保法》”）要求，针对个人信息主体及其相关方在数据授权平台上进行的数据授权行为，制定本办法。

第二条 在涉及个人信息的数据流通交易场景中，主要包括以下四方角色：数据提供方、个人信息主体、数据使用方和数据授权平台方。其中，数据提供方负责提供其合法合规收集到的个人信息数据，数据使用方则需通过数据授权平台获取个人信息主体的授权，并在授权范围内进行数据的合法使用。

（一）数据提供方是指合法持有或有权使用个人信息数据并在数据授权平台上提供这些数据的各类主体。数据提供方对其提供数据的质量负责，并且在数据的收集和处理过程中，严格遵守相关法律法规的要求。

（二）数据授权平台是一个技术与业务平台（以下简称“平台”），旨在为数据提供方、个人信息主体和数据使用方提供一个交互的界面，以便进行个人信息的授权和管理。平台提供用户友好的操作界面，并负责监督个人信息的授权过程，以确保授权过程符合《个保法》《数据授权平台用户协议》（以下简称“《用户协议》”）和《数据授权平台隐私政策》（以下简称“《隐私政策》”）的有关要求。

（三）个人信息主体，在平台的身份为授权人，依法享有对个人信息数据使用与处理的决定权，包括但不限于个人信息数据使用与否、使用条件、使用目的及适用场景等。为实现上述权益，个人信息主体可以通过数据授权平台进行数据授权、消息传递、个人信息管理、查询使用记录等活动。

（四）数据使用方，在平台的身份为被授权人，是指出于特定目的需要访问和使用个人信息的各类主体。数据使用方必须遵守数据授权平台中授权文件的有关规定，确保在授权范围内使用个人信息数据，并承担保护数据的安全和隐私的责任。

第二章　个人信息主体的权利和义务

第三条 个人信息主体对其个人信息的处理享有知情权、决定权和收益权，有权限制或者拒绝他人对其个人信息进行处理。法律、行政法规另有规定的除外。

第四条 个人信息主体有权查阅、复制其个人信息，并有权要求平台更正、补充或删除与其相关的个人信息数据，以确保数据的准确性和完整性。

第五条 对于平台经过个人信息主体同意而进行的个人信息处理，个人信息主体有权撤回已同意的授权。

第六条 个人信息主体有权向平台投诉未按照数据授权平台中的授权使用个人信息的行为。

第七条 个人信息主体在授权个人信息使用时，应仔细阅读并理解数据授权平台中授权文件的有关规定，了解平台及数据使用方的名称和联系方式、个人信息的处理目的、处理方式、所授权使用的个人信息种类、保存期限、行使权利的方式和程序，核对数据提供方所提供的相关个人信息的真实、准确性。

第三章　数据提供方的授权采集与接入

第八条 数据提供方在数据采集活动中，应当依据《个保法》做到个人信息的合法合规收集，通过书面方式（如《隐私政策》）向个人信息主体明确告知其收集个人信息

的目的、范围方式和个人信息种类、保存期限，并获得个人信息主体的明确同意。同时，应严格遵循最小必要原则，仅收集与特定目的直接相关且必要的数据，避免过度收集。

第九条 数据提供方应当采取必要的技术和管理措施，以保障数据的安全性，防止数据泄露和滥用；定期评估和审核数据收集活动，确保其持续符合法律法规要求。

第十条 数据提供方应实施恰当的技术和管理手段，以保障数据的安全性，预防数据泄露与滥用现象的发生；同时，应定期对数据收集活动进行评估与审核，确保其始终符合相关法律法规的规定。

第十一条 数据提供方有权决定是否将经个人信息主体授权采集到的个人信息加工后的数据产品接入到数据授权平台。同时有权设定数据分享的条件和范围。

第四章 数据使用方对个人信息的使用和处理

第十二条 数据使用方需要明确个人信息数据使用的目的和范围，在确保通过数据授权平台获得个人信息主体的明确同意和授权后进行数据的使用和处理。

第十三条 在申请数据使用授权的过程中，数据使用方应遵循透明度原则，以显著方式、清晰易懂的语言，向个人信息主体真实、准确、完整地披露被授权方的名称和联系方式、涉及的个人信息类型、使用场景、授权期限等相关信息。

第十四条 数据使用方在使用数据时，不得超出授权范围使用个人信息，应采取适当的保护措施，防止数据泄露，同时在数据使用过程中，尊重个人信息主体的数据权益和其他相关权利。

第五章 数据授权平台个人信息授权过程

第十五条 数据提供方同意将经个人信息主体授权后采集的个人信息所加工的数据产品接入数据授权平台后，按照平台规范进行技术对接，完成数据产品的平台对接与启用。

第十六条 数据使用方需根据数据授权平台所明确的信息类型列表，通过数据授权

平台提交详细的数据授权申请信息，包括但不限于拟使用数据的信息类型、最终使用者、使用目的、使用场景等信息，且申请信息必须明确标注授权的截止时间，并确保符合《个保法》等法律法规、《用户协议》及《隐私政策》的要求。

第十七条 数据授权平台接收到数据授权申请后，向个人信息主体发送授权请求，前述授权请求中包含授权范围、被授权人及所授权个人信息种类和授权期限的内容，以确保个人信息主体基于充分的了解做出明确的决定。

第十八条 若个人信息主体同意授权，将通过平台签署电子授权书，明确授权内容、授权期限等内容。经过个人信息主体同意的个人信息授权，个人信息主体可随时申请撤回其授权，已发生的费用和成本由撤回授权的个人信息主体承担，已交付给数据使用方的数据无法撤回，但平台可以通知数据使用方个人信息主体撤回授权的决定。

第六章 数据安全和隐私保护

第十九条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失：

（一）制定内部管理制度和操作规程；

（二）对个人信息实行分类管理；

（三）采取相应的加密、去标识化等安全技术措施；

（四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训；

（五）制定并组织实施个人信息安全事件应急预案；

（六）法律、行政法规规定的其他措施。

第二十条 履行个人信息保护职责的部门履行下列个人信息保护职责：

（一）开展个人信息保护宣传教育，指导、监督个人信息处理者开展个人信息保护工作；

（二）接受、处理与个人信息保护有关的投诉、举报；

（三）组织对应用程序等个人信息保护情况进行测评，并公布测评结果；

（四）调查、处理违法个人信息处理活动；

（五）法律、行政法规规定的其他职责。

第二十一条 在数据授权流通交易全部环节中，个人信息在存储和传输过程中应当进行加密。数据传输应采用安全协议，如传输层安全协议（Transport Layer Security）或安全套接层协议（Secure Sockets Layer），确保在互联网传输过程中的安全性。对于个人敏感数据，如个人财务信息或个人身份信息，应采用高级别的加密措施和专门的安全通道。

第二十二条 所有数据处理相关方的处理活动中，涉及的平台和工具必须通过多因素身份验证，包括密码、生物识别或手机令牌等方式才可允许访问，同时实施严格的访问控制策略，确保只有授权用户才能访问特定的数据集。平台方应定期审查访问日志，监控异常访问行为，并采取必要的预防措施。

第二十三条 为确保数据的安全性和可用性，备份策略应包括定期备份数据，选择合适的备份介质和存储位置，以及制定备份计划。恢复策略应明确恢复流程和步骤，测试备份数据的有效性，及时发现和解决潜在问题。同时，要建立备份恢复的监控和评估机制，不断优化策略，以适应业务变化和数据增长的需求。

第二十四条 除法律、行政法规另有规定外，个人信息的保存期限应当为实现特定处理目的所必要的最短期限内。

第七章 附则

第二十五条 本办法未尽事宜，按国家、北京市有关法律、法规、规章等规范性文件，以及数据授权平台用户协议及隐私政策的要求执行。本办法如与法律、法规、规范性文件、平台用户协议及隐私政策不一致的，以法律、法规、规范性文件、平台用户协议及隐私政策的规定为准。

第二十六条 本办法由北京国际大数据交易所有限责任公司负责解释和修订。

第二十七条 本办法自发布之日起施行。

《国家网络身份认证公共服务管理办法（征求意见稿）》

发文机关：公安部、国家互联网信息办公室

发布时间：2024.07.26

生效时间：待定

第一条 为实施网络可信身份战略，推进国家网络身份认证公共服务建设，保护公民身份信息安全，促进数字经济发展，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《中华人民共和国反电信网络诈骗法》等法律法规，制定本办法。

第二条 本办法所称国家网络身份认证公共服务（以下称“公共服务”），是指国家根据法定身份证件信息，依托国家统一建设的网络身份认证公共服务平台（以下称“公共服务平台”），为自然人提供申领网号、网证以及进行身份核验等服务。

本办法所称网号，是指与自然人身份信息一一对应，由字母和数字组成、不含明文身份信息的网络身份符号；网证，是指承载网号及自然人非明文身份信息的网络身份认证凭证。网号、网证可用于在互联网服务及有关部门、行业管理、服务中非明文登记、核验自然人真实身份信息。

第三条 国务院公安部门、国家网信部门依照各自法定职责，负责国家网络身份认证公共服务的监督管理，监督、指导公共服务平台依法落实数据安全和个人信息保护义务。

国务院民政、文化和旅游、广播电视、卫生健康、铁路、邮政等部门依照本办法和有关法律、行政法规的规定，在各自职责范围内负责国家网络身份认证公共服务的推广应用和监督管理工作。

第四条 持有有效法定身份证件的自然人，可自愿向公共服务平台申领网号、网证。

不满十四周岁的自然人需要申领网号、网证的，应当征得其父母或者其他监护人同意，并由其父母或者其他监护人代为申领。

已满十四周岁未满十八周岁的自然人需要申领网号、网证的，应当在其父母或者其

他监护人的监护下申领。

第五条 根据法律、行政法规规定，在互联网服务中需要登记、核验用户真实身份信息的，可以使用网号、网证依法进行登记、核验。

不满十四周岁的自然人使用网号、网证登记、核验真实身份信息的，应当征得其父母或者其他监护人同意。

第六条 鼓励有关主管部门、重点行业按照自愿原则推广应用网号、网证，为用户提供安全、便捷的身份登记和核验服务，通过公共服务培育网络身份认证应用生态。

第七条 鼓励互联网平台按照自愿原则接入公共服务，用以支持用户使用网号、网证登记、核验用户真实身份信息，依法履行个人信息保护和核验用户真实身份信息的义务。

互联网平台接入公共服务后，用户选择使用网号、网证登记、核验真实身份信息并通过验证的，互联网平台不得要求用户另行提供明文身份信息，法律、行政法规另有规定或者用户同意提供的除外。

互联网平台应当保障使用网号、网证的用户与其他用户享有相同服务。

第八条 互联网平台需要依法核验用户真实身份信息但无需留存用户法定身份证件信息的，公共服务平台应当仅提供用户身份核验结果。

根据法律、行政法规规定，互联网平台确需获取、留存用户法定身份证件信息的，经用户授权或者单独同意，公共服务平台应当按照最小化原则提供。

未经自然人单独同意，互联网平台不得擅自处理或者对外提供相关数据信息，法律、行政法规另有规定的除外。

第九条 公共服务平台处理个人信息不得超出为自然人提供申领网号、网证以及进行身份核验等服务所必需的范围和限度，在向自然人提供公共服务时应当依法履行告知义务并取得其同意。处理敏感个人信息的，应当取得个人的单独同意，法律、行政法规规定应当取得书面同意的，从其规定。

未经自然人单独同意，公共服务平台不得擅自处理或者对外提供相关数据信息，法律、行政法规另有规定的除外。

公共服务平台应当依照法律、行政法规规定或者用户要求，及时删除用户个人信息。

第十条 公共服务平台在处理用户个人信息前，应当通过用户协议等书面形式，以显著方式、清晰易懂的语言真实、准确、完整地向用户告知下列事项：

（一）公共服务平台的名称和联系方式；

（二）用户个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）用户依法行使其个人信息相关权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

处理敏感个人信息的，还应当向个人告知处理的必要性以及对个人权益的影响，法律、行政法规另有规定的除外。

第十一条 公共服务平台处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知前条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，公共服务平台应当在紧急情况消除后及时告知。

第十二条 公共服务平台应当加强数据安全和个人信息保护，依法建立并落实安全管理制度与技术防护措施。

第十三条 公共服务平台的建设和服务涉及密码的，应当符合国家密码管理有关要求。

第十四条 违反本办法第七条第二款、第八条、第九条、第十条、第十二条规定，依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》应当追究法律责任的，由国务院公安部门、国家网信部门在各自职责范围内依法予以处罚；构成犯罪的，依法追究刑事责任。

第十五条 本办法所称法定身份证件，包括居民身份证、定居国外的中国公民的护照、前往港澳通行证、港澳居民来往内地通行证、台湾居民来往大陆通行证、港澳居民居住证、台湾居民居住证、外国人永久居留身份证等身份证件。

第十六条本办法自 年 月 日起施行。

二、数安热点

1. 最高院司法案例研究院发布侵犯公民个人信息罪相关案例裁判要旨汇总

（1）指导性案例 193 号：闻巍等侵犯公民个人信息案

裁判要点：居民身份证信息包含自然人姓名、人脸识别信息、身份号码、户籍地址等多种个人信息，属于《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第五条第一款第四项规定的“其他可能影响人身、财产安全的公民个人信息”。非法获取、出售或者提供居民身份证信息，情节严重的，依照刑法第二百五十三条之一第一款规定，构成侵犯公民个人信息罪。

（2）指导性案例 194 号：熊昌恒等侵犯公民个人信息案

裁判要点：1.违反国家有关规定，购买已注册但未使用的微信账号等社交媒体账号，通过具有智能群发、添加好友、建立讨论群组等功能的营销软件，非法制作带有公民个人信息可用于社交活动的微信账号等社交媒体账号出售、提供给他人，情节严重的，属于刑法第二百五十三条之一第一款规定的“违反国家有关规定，向他人出售或者提供公民个人信息”行为，构成侵犯公民个人信息罪。2.未经公民本人同意，或未具备具有法律授权等个人信息保护法规定的理由，通过购买、收受、交换等方式获取在一定范围内已公开的公民个人信息进行非法利用，改变了公民公开个人信息的范围、目的和用途，不属于法律规定的合理处理，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”行为，情节严重的，构成侵犯公民个人信息罪。

（3）刘某某侵犯公民个人信息案

裁判要旨：向不特定多数人发布公民个人信息，情节严重，符合刑法第二百五十三条之一规定的，构成侵犯公民个人信息罪。司法实践中，对通过“人肉搜索”“开盒”

等方式，在网络上非法曝光他人隐私、发布公民个人信息等网络暴力行为，可以依法适用侵犯公民个人信息罪的规定。

（4）夏某晓侵犯公民个人信息案

裁判要旨：1.非法买卖公民个人信息，属于刑法第二百五十三条之一规定的“非法获取公民个人信息”“出售公民个人信息”，情节严重的，应当以侵犯公民个人信息罪论处。2.网购订单信息与财产安全直接相关，属于敏感信息的范畴，可以归入《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号）第五条规定的“交易信息”。

（5）林某侵犯公民个人信息案

裁判要旨：违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，构成侵犯公民个人信息罪。通过刑事附带民事公益诉讼，对被告人实施刑事和民事双重制裁，更有利于实现对公民个人信息的保护。

（6）周某城侵犯公民个人信息案

裁判要旨：1.非法购买公民个人信息出售牟利，属于刑法第二百五十三条之一规定的“非法获取公民个人信息”“出售公民个人信息”，情节严重的，应当以侵犯公民个人信息罪论处。2.非法购买公民个人信息后又出售的，公民个人信息的条数不重复计算。

（7）赵某岗侵犯公民个人信息案

裁判要旨：办理侵犯公民个人信息刑事案件，对于非法获取的公民个人信息数量庞大的，应当进行查重处理，对重复部分予以扣减，并据此定罪量刑。

（8）王某侵犯公民个人信息案

裁判要旨：《民法典》第一千零三十六条规定:“处理个人信息,有下列情形之一的,行

为人不承担民事责任:……(二)合理处理该自然人自行公开的或者其他已经合法公开的信息,但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外……”(《个人信息保护法》第十三条、第二十七条有类似规定)据此,对公开的个人信息的合理处理可以推定自然人概括同意,即除了“该自然人明确拒绝或者处理该信息侵害其重大利益的”情形外,不需要通知和征得该自然人或者其监护人同意。故而，对于自行公开的或者其他已经合法公开的个人信息，行为人获取相关信息后出售、提供的行为，一般不宜以侵犯公民个人信息罪论处。本案虽然系 2019 年作出的判决,但所把握的精神与《民法典》《个人信息保护法》对公开信息的相关规定是一致的。

（9）王某侵犯公民个人信息案

裁判要旨：公民个人信息是动态且高度依赖于具体场景的，仅机械适用“概括＋列举”方式静态类型化识别并不符合实际，故必须结合个案情况进行动态认定，即应结合具体案件因素对信息来源、去处、种类、价值以及其与人身权、财产权的紧密程度等综合加以判定。对于侵犯了单一信息如电话号码、购物信息等的，应当判断该信息是否关联人身利益与财产利益，对案涉信息进行限缩解释，从而避免无限递归下的动辄得咎。对于具有较高识别能力的个人和企业，应当根据其客观能力、义务范围等综合判定其对信息的可识别性。因此，对公民个人信息除以可识别性作为本质认定标准外，还应当综合考虑行为人的行为方式及侵犯公民个人信息的种类、数量、危害后果、识别能力等因素，对案涉信息进行动态识别。

（10）卢某某侵犯公民个人信息案

裁判要旨：1.房产信息是否属于侵犯公民个人信息犯罪中的财产信息不应一概而论。判断房产信息是否属于本罪中的财产信息，关键在于该信息是否直接涉及公民个人人身财产安全。2.判断涉案房产信息是否属于“财产信息”的范畴，坚持主客观相统一原则，以信息流向作为信息类型归属的重要判断因素。涉案房产信息被房屋中介公司、装修公司工作人员购买，用于业务推广的，通常不会影响人身财产安全，一般不宜认定为财产信息。

（11）邱某某侵犯公民个人信息案

裁判要旨：1.行踪轨迹信息能够实时反映相关人员的轨迹状况，与人身安全直接相关，系高度敏感信息，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号）第五条将入罪标准设置为“五十条以上”，升档量刑标准设置为“五百条以上”。2.对于行踪轨迹信息的认定，原则上只宜理解为 GPS 定位信息、车辆轨迹信息等可以直接定位特定自然人具体坐标的信息。本案所涉及的通过车载 GPS 定位器获取的定位信息，应当纳入行踪轨迹信息的范畴。3.行踪轨迹信息不等于涉及轨迹的信息，而应当理解为涉及轨迹的实时信息。广义上而言，涉及轨迹的信息范围较宽，诸如火车票信息、机票信息等相关轨迹信息并非实时信息，故应当排除在行踪轨迹信息的范围之外。与之不同，本案所涉车辆定位信息则均属于实时信息的范畴，应当认定为行踪轨迹信息。

（12）钱某勇、王某春等侵犯公民个人信息案

裁判要旨：1.财产信息与财产安全直接相关，系高度敏感信息，《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（法释〔2017〕10 号）第五条将入罪标准设置为“五十条以上”，升档量刑标准设置为“五百条以上”。2.房产信息是否属于侵犯公民个人信息犯罪中的财产信息不应一概而论。判断房产信息是否属于本罪中的财产信息，关键在于该信息是否直接涉及公民个人人身财产安全。“公民个人房屋权籍调查信息”直接来源于银行房屋信息系统，属于直接反映财产状况的信息，涉及财产安全，可以纳入“财产信息”的范畴。3.判断涉案信息是否属于“财产信息”的范畴，可以结合信息获取渠道和交易价格考量。司法实践中，作为佐证，可以将信息交易价格作为敏感信息判断的辅助因素。通常而言，敏感信息、特别是高度敏感信息的交易价格要远远高于一般公民个人信息。

（13）刘某侵犯公民个人信息案

裁判要旨：侵犯公民个人信息罪中“公民个人信息”的认定，应当强调身份的可识别性以及与人身、财产法益的关联性，判断是否具备形式的可识别性、内容的隐私性、来源的不公开性、性质的敏感性等四项特征。对于非法获取公民个人信息，违法所得 5 万元以上的，除为合法经营活动非法购买、收受外，应认定为“情节特别严重”。

（14）秦某乐等人侵犯公民个人信息案

裁判要旨：1.在侵犯公民个人信息刑事附带民事公益诉讼案件中，民事主体因同一行为应当承担民事责任、行政责任和刑事责任的，承担行政责任或者刑事责任不影响承担民事责任。因此，追缴违法所得和公益损害赔偿可以并存。2.在侵犯公民个人信息刑事附带民事公益诉讼案件中，行为人侵犯了不特定公民的信息权益，可以按照民法典第一百七十九条的规定承担相应的民事责任，并依据民法典第一千一百二十八条、个人信息保护法第六十九条的规定确定损害赔偿的数额。被告人违法所得数额是从犯罪中获得的收益，依据实际查明的获利数额进行追缴。如果实际损失数额能够查清，可以依据实际损失来认定。如果实际损失或者获利数额都无法查清，法院可以视情况酌定损害赔偿的数额。

（15）郭某、吕某等侵犯公民个人信息案

裁判要旨：1.检察机关就侵犯公民个人信息的犯罪行为能否提起附带民事公益诉讼问题。侵犯公民个人信息的行为，可能造成不特定社会公众的个人信息更广泛地泄露和传播，滋生电信网络诈骗、“套路贷”等下游犯罪，进而威胁公众人身、财产安全，侵害了公共利益。保护公民个人信息事关不特定公众群体的切身利益，具有公益属性。检察机关在起诉实施侵犯公民个人信息行为的被告人时，可同时提起附带民事公益诉讼，符合国家对公民个人信息保护的价值取向，弥补了个人信息保护私益诉讼的不足。2.同时科处刑事责任和民事责任是否竞合的问题。刑事责任与民事责任本质目的均为保护法益，但二者保护的法益并不相同，刑事责任是对违法行为人的惩罚和制裁，民事责任是对受害人所受损害的补救。二者内在逻辑存在本质区别，功能、性质均不相同，不存在冲突，相互不能被吸收，更无法替代。通过刑事

附带民事公益诉讼，被告人除应承担刑事责任外，还应承担赔偿损失、向公众赔礼道歉、消除危险等民事责任。对被告人实施刑事和民事双重制裁，形成追责合力，更有利于实现对违法行为的预防和对公益的全面保护。

（16）陈某展等 17 人诈骗、敲诈勒索、侵犯公民个人信息案

裁判要旨：“套路贷”案件中，认定财务人员将逾期借款人名单移交给催收人员是否构成敲诈勒索罪共犯，应当综合考虑被告人的具体犯意内容、收益情况、参与共同犯罪的意思联络等情节，如财务人员与催收人员认识因素和犯罪目标不一致，犯意联络不明显，犯罪所得利益没有共享，可以不认定财务人员构成敲诈勒索罪的共犯。

（17）谢某某侵犯公民个人信息、非法获取计算机信息系统数据案

裁判要旨：公民个人电子信息通常表现为计算机信息系统数据。违反国家规定侵入计算机信息系统，或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的个人信息，同时符合了侵犯公民个人信息罪与非法获取计算机信息系统数据罪两个犯罪构成，但由于只有一个犯罪行为，属于刑法中的想象竞合犯，应当从一重罪处断；两罪法定刑相同时，可以按照侵犯公民个人信息罪定罪处罚。

（18）吴某某等盗窃、侵犯公民个人信息、帮助信息网络犯罪活动案

裁判要旨：行为人利用信息网络，诱骗他人点击虚假链接，通过预先设置的程序窃取他人财物的，应当以盗窃罪定罪处罚。对既采取“秘密窃取手段”又采取“欺骗手段”非法占有财物行为的定性，应从行为人采取主要手段和被害人有无处分财物意识方面区分盗窃与诈骗。如果行为人获取财物时起决定性作用的手段是“秘密窃取”，“虚构事实、隐瞒真相”只是为了转移被害人注意力或使被害人无法察觉，是为盗窃创造条件或作掩护，被害人也没有自愿交付财物的，就应当认定为盗窃；如果行为人获取财物时起决定性作用的手段是“诈骗”，被害人基于错误认识而自愿交付财物，“盗窃行为”只是辅助手段的，就应当认定为诈骗。

2. 六家咖啡企业依然存在违规采集消费者个人信息问题，被上海市网信办会同市市场监管局依法约谈

日前，上海市网信办会同市市场监管局组织开展“咖啡消费场景下个人信息保护”专项整治活动。近日，上海市网信办在进行复核检查时发现，太平洋咖啡、瑞幸咖啡、COSTA COFFEE、M Stand、挪瓦咖啡和一尺花园等六家咖啡企业在个人信息保护方面仍存在整改不力的问题，这表明这些企业尚未充分遵守《个人信息保护法》的相关规定，在 8 月 6 日下午联合市场监管局依法对这些企业的负责人进行了约谈。在约谈过程中，上海市网信办严肃指出了这些企业在隐私政策方面存在的问题，包括隐私政策的缺失、不准确或不完整，以及在收集用户精确位置信息、强制或诱导用户注册会员、未提供关闭个性化推送等方面存在的违规行为。网信办要求这些企业必须认真执行个人信息保护的责任，严格遵循个人信息处理的"最小必要"原则和"告知-同意"原则，确保隐私政策的透明度和完整性，以及个人信息收集的合法合规性。同时，市场监管局也要求这些企业采取切实有效的措施来保护消费者的合法权益，遵守《消费者权益保护法》及其实施条例的相关规定，承担起企业对消费者个人信息保护的主体责任，确保企业的合法合规经营和规范经营。

3. 消费者差评遭霸王茶姬员工上门请求删除或侵犯消费者个人信息

近日，茶饮品牌“霸王茶姬”因员工上门请求顾客删除差评而引发争议。一名成都顾客在给霸王茶姬的饮品差评后，遭到门店员工上门要求删除差评，该员工还提供了额外的饮品和徽章作为补偿。此事在网上引发热议，许多网友对门店员工获取顾客住址的方式表示担忧，认为这可能侵犯了消费者的个人信息安全。江苏省消费者权益保护委员会对此事发声，认为霸王茶姬的行为涉嫌侵犯消费者的知情权和监督权，呼吁商家应尊重消费者的差评权，通过消费者的反馈找出问题根源，不断提升品牌和服务。

4. 审计署发布 2024 年第 1 号公告：四部委所属 7 家单位利用政务数据违规牟利 2.48 亿元

6 月 25 日，审计署发布关于中央部门单位 2023 年预算执行和其他相关情况的审计结果。公告显示，在 2023 年 11 月至 2024 年 2 月期间，审计署对 41 个部门及其 346 家单位的财政预算拨款进行了重点审计，涉及金额达到 5824.04 亿元。审计过程中共发现了各类问题金额 226.26 亿元，其中部门本级涉及金额 36.29 亿元，所属单位则为 189.97 亿元。具体涉及部门与违规情况如下：

- 交通运输部：2018 年 6 月至 2023 年，所属 2 家单位下属企业利用 4 个信息系统政务数据违规收费 1.45 亿元，其中 2023 年 5183.37 万元。
- 教育部：2018 年至 2023 年，所属 2 家单位违规利用 3 个信息系统政务数据收费 5865.7 万元。
- 工业和信息化部：2020 年至 2023 年，所属 2 家单位利用 5 个信息系统政务数据违规收费 2447.07 万元，其中 2023 年 713.03 万元。
- 市场监管总局：2019 年 12 月至 2023 年，所属 1 家单位下属企业违规利用 1 个信息系统政务数据收费 2024.55 万元。

5. 首例涉及《数据知识产权登记证》司法效力案宣判

上诉人隐木(上海)科技有限公司因与被上诉人数据堂(北京)科技股份有限公司不正当竞争纠纷一案为首例涉及《数据知识产权登记证》司法效力的案件。近日，北京知识产权法院确认了该证书的初步证据效力，并判决隐木（上海）科技有限公司（隐木公司）构成不正当竞争，需赔偿数据堂（北京）科技股份有限公司（数据堂公司）经济损失 10 万元。

案件背景：数据堂公司收集并整理了 1505 小时的普通话语音数据 aidatatang-1505zh，并向高校和学术机构等非商业组织开源提供，同时通过授权第三方使用获得收益。隐木公司通过开源途径获取其中的 200 小时数据集进行商业性使用，双方因此产生

争议。

法院认为：《数据知识产权登记证》可作为证明数据堂公司享有涉案数据集相关财产性利益的初步证据，亦可作为涉案数据集收集行为合法的初步证据。这一判决强化了《数据知识产权登记证》的权威性，为日后解决数据权属纠纷、明确权属关系提供了可借鉴的司法实践参考。

此外，法院还指出，数据集应当具有实质数量的数据条目才能获得保护，以避免对普通公众的创作和表达自由产生负面影响。最终，隐木公司被判构成不正当竞争，需赔偿数据堂公司经济损失 10 万元。