

2021

天达共和数据合规资讯月报



No. 01

天达共和数据合规团队

摘要

尊敬的各位客户、同仁：

欢迎参阅天达共和律师事务所数据合规团队为您呈现的《数据合规资讯月报》2021 年第一期，本期月报主要内容包括：

- **立法动态**

介绍 2020 年 12 月 26 日至 2021 年 01 月 25 日期间及前后境内外数据保护立法动态，并针对部分立法动态提供简要评论。

- **执法聚焦**

介绍 2020 年 12 月 26 日至 2021 年 01 月 25 日期间及前后境内外部分典型执法案例，并针对部分执法活动提供简要评论。

- **行业新闻**

精选 2020 年 12 月 26 日至 2021 年 01 月 25 日期间及前后互联网及相关行业与网络安全和数据保护有关的新闻资讯。

- **热点评述**

在本期月报中，我们将和您分享本团队题为《从拼多多辞退匿名发帖员工看员工与用人单位使用社交媒体的法律风险》的文章。该文章从拼多多辞退匿名发帖员工热点事件出发，探讨了员工言论自由的边界，并就用人单位涉互联网媒体使用方面提出合规建议，欢迎阅览参考。

目 录

摘 要	1
目 录	2
立 法 动 态	3
➢ 境内立法	3
➢ 境外立法	8
执 法 聚 焦	10
➢ 境内执法	10
➢ 境外执法	12
行 业 新 闻	14
➢ 境内新闻	14
➢ 境外新闻	14
热 点 评 述	16

立法动态

境内立法

- 12月26日，第十三届全国人民代表大会常务委员会第二十四次会议通过了《中华人民共和国刑法修正案（十一）》（“刑修十一”），并自2021年3月1日起施行。刑修十一在刑法第一百三十四条后增加一条，作为第一百三十四条之一，明确了**在生产、作业中违反安全管理规定，有关闭、破坏直接关系生产安全的监控、报警、防护、救生设备、设施，或者篡改、隐瞒、销毁其相关数据、信息情形的，具有发生重大伤亡事故或者其他严重后果的现实危险的，可处一年以下有期徒刑、拘役或者管制。**

<http://www.npc.gov.cn/npc/c30834/202012/850abff47854495e9871997bf64803b6.shtml>

简析：第一百三十四条之一的具体罪名尚不得知，但从刑修十一可看出这个新增的罪涉及违反安全管理规定，并且属于无需造成后果，只要存在发生重大伤亡事故或其他严重后果的现实危险即构成犯罪。刑修十一将数据、信息安全纳入刑法规制体系，将进一步促进工业互联网安全体系的构建，为工业信息化建设提供上位法保障。具有重要系统的工业类企业有必要特别关注系统内有关重要数据、信息的安全性，否则可能触发刑事责任风险。

- 1月5日，全国信息安全标准化技术委员会（“信安标委”）发布《网络安全标准实践指南—人工智能伦理安全风险防范指引》。该实践指南的出台背景为，人工智能迅速发展的同时，带来了诸多伦理安全风险，包括影响社会价值、侵犯个人权利等。该实践指南依据法律法规要求及社会价值观，针对人工智能的伦理安全风险，给出了安全风险防范措施，为人工智能研发、设计制造、部署应用等提供指引。人工智能的伦理安全风险防范的基本要求包括尊重并保护个人基本权利，包括人身、隐私、财产等权利，特别关注保护弱势群体；在设计制造方面，不应设计损害公共利益或个人权利的人工智能系统、产品或服务；在部署应用方面，使用人工智能作为直接决策依据并影响个人权利时，应具有清晰、明确、可查的法律法规等依据；在用户使用方面，不应以有损社会价值、个人权利等目的恶意使用人工智能。

<https://mp.weixin.qq.com/s/NwvWkvGECtnAigCmxtZxmw>

简析：人工智能的部署应用，可能涉及自动化决策机制，这与个人信息保护方面的自动化决策机制密切相关或者说可能在指向上具有同一性。人工智能的孕育本身需要大量数据的“投喂”用于练习，数据是人工智能的“血液”，但是人工智能的应用反过来会经由对数据的分析带来侵害特定个人权益或不特定个人权益方面的影响。该实践指南为人工智能的良性发展指明了方向，积聚了海量数据的企业开展算法研究、应用或人工智能研究、应用，有必要参照借鉴该实践指南。

- 1月5日，中国银行保险监督管理委员会（“银保监会”）发布了《保险中介机构信息化工作监管办法》（“《办法》”），自2021年2月1日起施行。《办法》共6章36条，在规定了保险中介机构的信息化工作机构职责、关联企业隔离要求、监管报送要求、突发事件报告等基本要求的同时，从信息系统建设、信息安全要求、信息化工作的监督管理等方面对保险中介机构信息化工作提出了全面要求。（1）人员配备方面，保险中

介法人机构应设置信息化部门或信息化岗位，负责信息化工作的正式工作人员不少于一人。（2）向监管部门报送信息方面，申请开展保险中介业务的法人机构应向机构营业执照登记注册地银保监会派出机构报送信息化工作情况报告，**报告内容应包括信息化管理机制和制度情况、信息系统满足《办法》第十七条要求的情况、信息系统采购合同或知识产权证书等。**（3）信息系统建设方式方面，保险中介机构可采取自主开发、合作开发、定制开发、外包开发和购买云服务等形式建设信息系统，其中**非自主研发建设信息系统的，保险中介机构应识别和分析信息科技外包风险，加强对外包服务商的资质审查和风险管理，规范外包合同条款，采取有效手段保障数据和信息系统安全且持续可控。**（4）信息安全方面，保险中介机构应建立健全信息安全管理制，实施网络安全等级保护，确定网络安全等级并按相应标准进行防护；对重要数据采取保护措施；采取可靠措施进行数据存储和备份，定期开展备份数据恢复验证；**系统数据应至少保存五年，系统日志应至少保存六个月；收集、处理和应用数据涉及到个人信息的，应遵循合法、正当、必要的原则，遵守国家相关法律、行政法规，符合与个人信息安全相关的国家标准；**应加强对台式计算机、便携式计算机、智能手机、平板电脑、移动存储介质等终端设备的管理；**应经常开展信息化培训、信息安全培训和保密教育，与员工签订信息安全和保密协议，督促员工履行与其工作岗位相应的信息安全和保密职责；**（5）监督管理方面，不符合《办法》要求的视为不满足《保险代理人监管规定》《保险经纪人监管规定》《保险公估人监管规定》对于信息化建设和管理的相关规定，不得经营保险中介业务。此外，保险中介机构应按照《办法》进行信息化工作自查，在《办法》实施之日起一年内完成整改。

（<http://www.cbirc.gov.cn/cn/view/pages/governmentDetail.html?docId=958343&itemId=861&generalType=1>）

简析：（1）虽然《办法》提及保险中介机构遵守个人信息安全相关国家标准时，没有指明相关国家标准是否仅指强制性国家标准，还是指包括推荐性国家标准，但这释放了一个非常强烈的信号：有关行业主管部门如银保监会将以有关个人信息的国家标准作为评判保险中介机构合法性的标准之一。保险中介机构有必要对照《信息安全技术 个人信息安全规范》（GB/T 35273-2020）等国家标准梳理企业运营所涉个人信息处理是否合规，如有不合规之处，尽快整改。（2）《网络安全法》将实施网络安全等级保护制度要求提升到法律层面，《办法》则体现了行业监管部门在行业内贯彻执行网络安全等级保护制度的决心。（3）保险中介机构须与员工签订信息安全和保密协议，并应经常开展信息化培训、信息安全培训和保密教育。为应对监管部门的检查，保险中介机构有必要将培训材料、培训开展的记录存档备查。（4）保险中介机构不符合《办法》规定，不得经营保险中介义务，这意味着保险中介机构必须在一年内完成整改。尚未达到《办法》要求的保险中介机构不仅需要从信息系统建设的技术方面，也要从内部管理制度、流程和有关配套文本方面全面整改以符合《办法》确定的合规要求，从而确保持续营业的可能性。

- 1月7日，为规范创业板上市公司从事通信、网络安全相关业务的信息披露行为，保护投资者的合法权益，深圳证券交易所制定并发布了《深圳证券交易所创业板行业信息披露指引第14号——上市公司从事通信相关业务》《深圳证券交易所创业板行业信息披露指引第15号——上市公司从事网络安全相关业务》，并于发布之日起施行。

(http://www.szse.cn/lawrules/rule/gem/t20210108_584158.html)

简析：我国创业板已聚集了一批通信、网络安全企业，引起市场上的高度关注，此次指引的发布施行明确了行业信息披露要求。

- 1月8日，为促进互联网信息服务健康有序发展，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，国家互联网信息办公室（“网信办”）会同工业和信息化部（“工信部”）、公安部起草了《互联网信息服务管理办法（修订草案征求意见稿）》（“征求意见稿”），并公开向社会征求意见。征求意见稿中增加了域外适用的情形，中华人民共和国境内的任何组织和个人利用境内外网络资源向境内用户提供互联网信息服务，应当遵守该办法规定；明确了执法部门及其具体分工。对于新闻、文化、出版、视听节目、教育、医疗保健、药品和医疗器械这些特殊领域作出了更具体的规定，从事互联网新闻信息服务，应当向网信部门提出申请；从事文化、出版、视听节目的互联网信息服务，应当取得有关部门的许可；从事教育、医疗保健、药品和医疗器械等互联网信息服务，依照法律、行政法规以及国务院有关规定须经有关部门许可的，应当取得有关部门的许可。从事互联网信息服务，属于经营电信业务的，应当取得电信主管部门电信业务经营许可；不属于经营电信业务的，应当在电信主管部门备案。未取得电信业务经营许可或者未履行备案手续的，不得从事互联网信息服务。与此同时，征求意见稿与《网络安全法》等网络、数据安全立法进行衔接，结合近年来互联网发展中出现的新问题，进行了更为具体且具有针对性的规定。

(http://www.cac.gov.cn/2021-01/08/c_1611676476075132.htm)

简析：《互联网信息服务管理办法》是我国互联网管理方面的基础性法规，自2000年实施，2011年有过一次修订。此次征求意见稿扩大了以往通常理解的互联网信息服务类型的范围，明确将网络支付、广告推广、网络存储等列为互联网信息服务，可能涉及未来该管理办法出台后是否需要取得B25类许可证的问题。企业未来需要比照正式通过的管理办法界定自己的经营业态是否属于互联网信息服务，取得电信业务经营许可或备案，否则将影响业务能否持续开展。

- 1月11日，为营造更好的测试示范环境，共促智能网联汽车产业生态健康发展，工信部会同公安部、交通运输部组织行业机构、重点企业等开展《智能网联汽车道路测试与示范应用管理规范（试行）》的修订并形成征求意见稿，现公开征求社会各界意见。征求意见稿截止日期为2021年2月11日。

(https://www.miit.gov.cn/jgsj/zbys/qcgy/art/2021/art_729754f35bb4429f92be987c0cc196e3.html)

- 1月12日，为贯彻落实国务院常务会议关于促进征信业发展提质、建立健全征信体系的会议精神，坚持征信为民，规范征信业务及其相关活动，加强征信监督管理，促进征信业健康发展，中国人民银行（“人民银行”）草拟了《征信业务管理办法（征求意见稿）》（“征求意见稿”），并向社会公开征求意见，意见反馈截止时间为2021年2月10日。

（1）该征求意见稿规定了域外适用效力，即在境外对中国居民开展征信业务及相关活动，适用该管理办法。

(2) 征信机构采集信用信息方面：

(a) 应当遵循“最少、必要”的原则，不得过度采集，不得以欺骗、胁迫、诱导、以向被采集的个人或企业收费的方式、不得从非法渠道采集或以其他侵害信息主体合法权益的方式采集信用信息；

(b) 应对信息提供者的业务合法性、信息来源、信息质量、信息安全、信息主体授权等进行审核，保障采集信用信息的合法、准确和可持续性；

(c) **应经信息主体本人同意，并明确告知信息主体采集信用信息的目的、信息来源和信息范围**，以及不同意采集信息可能产生的不利后果等事项；

(d) 采集非公开的企业信用信息，应当采取适当的方式取得企业的同意。

(3) 在信用信息的使用和提供方面：

(a) 征信机构应当采取适当的措施，**对信息使用者的身份、业务资质、使用目的等进行必要的审查**；

(b) 征信机构应当对通过网络形式接入征信系统的信息使用者的网络和系统安全、合规性管理措施进行必要的审查，对查询行为进行监测，发现违规行为，及时停止服务；

(c) **征信机构应当对信息使用者进行必要的审查，保障信息使用者查询个人信息时获取信息主体同意、按照约定用途使用**；

(d) 信息使用者使用征信机构提供的信用信息，应当用于合法、正当的目的，不得滥用。**信息使用者使用个人信用信息应当有明确、具体的目的，按照与信息主体约定的用途使用，超出约定用途的，应当另行取得同意。**

(4) 在信用信息安全方面：

(a) **个人征信机构、保存或处理 50 万户以上企业信用信息的企业征信机构，其系统测评为国家信用信息安全等级保护三级或三级以上**，应设立信息安全负责人，由公司章程规定的高级管理人员担任；应设立专职部门，负责管理信息安全工作，定期检查有关业务及征信系统的管理制度及措施执行情况，等等；

(b) 征信机构应当严格限定查询、获取信用信息的工作人员的权限和范围。征信机构应当建立工作人员查询、获取信用信息的操作记录，明确记载工作人员查询、获取信用信息的时间、方式、内容及用途；

(c) **征信机构在中国境内开展征信业务及相关活动，生产数据库、备份数据库应设在中国境内**；

(d) **征信机构向境外提供个人信用信息，应当符合国家法律法规的规定；征信机构向境外提供企业信用信息查询服务，应当审查信息使用者的身份、用途，确保信用信息用于跨境贸易、融资等合理的用途，并采取单笔查询的方式提供。征信机构不得将某一区域、某一行业批量企业的信用信息传输至境外同一信息使用者。征信机构向境外提供企业信用信息的，应当向中国人民银行备案。征信机构与境外征信机构合作的，应当在合作协议签署后向中国人民银行备案。**

(http://www.gov.cn/xinwen/2021-01/12/content_5579283.htm)

简析：该征求意见稿对征信机构提出了更高的合规要求，对于征信机构的规范（如通过审核信息提供者的业务合法性、信息来源、信息主体授权等保障采集信用信息的合

法、准确和可持续性)和信用信息使用者的规范(如基于合法、正当的目的)将有助于提升对个人信用信息的保护水平。

该征求意见稿还对企业的信用信息加强了保护,尤其是境内存储数据要求以及不得将区域性、行业性批量企业信用信息传输至境外同一信息使用者,而应进行单笔查询,这可能对某些企业征信机构以及购买某些企业征信机构服务用于进一步向境外提供企业信息查询服务的企业运营带来影响。另,不允许批量提供查询企业信用信息与我国有关标准的征求意见稿中对重要数据的定义是相一致的,实际上,数据的量庞大到一定程度,不排除提炼出可能危害国家安全或社会公共利益的信息的可能性。

- 1月21日,为加强对非银行支付机构的监督管理,规范非银行支付机构行为,防范支付风险,保障当事人合法权益,促进支付服务市场健康发展,人民银行会同有关部门研究起草发布了《非银行支付机构条例(征求意见稿)》(以下称为“征求意见稿”),并向社会公开征求意见。意见反馈截止时间为2021年2月19日。根据该征求意见稿,从事支付交易处理业务的非银行支付机构应当根据清算机构、银行、从事储值账户运营业务的非银行支付机构认可的安全认证方式访问账户,不得留存账户敏感信息;非银行支付机构应当对足以影响用户是否同意使用支付服务的相关协议内容尽到信息披露义务;非银行支付机构收集、使用用户信息,应遵守个人信息保护的相关规定,如应当遵循合法、正当、必要的原则,公开收集、使用用户信息的规则,明示收集、使用用户信息的目的、方式和范围,并经用户明示同意等,不得将用户授权或者同意其将用户信息用于营销、对外提供等作为与用户建立业务关系的先决条件,但业务关系的性质决定需要预先作出相关授权或者同意的除外;非银行支付机构被认定为关键信息基础设施运营者的,其在中国境内收集和产生的用户信息的储存、处理和分析应当在境内进行。非银行支付机构向境外提供境内用户信息的,应当符合法律、行政法规、部门规章以及中国人民银行的规定,并经用户明示同意。

(http://www.gov.cn/xinwen/2021-01/21/content_5581574.htm)

简析:根据该征求意见稿,非银行支付机构如果被认定为关键信息基础设施经营者的,除了境内存储数据要求外,向境外提供境内用户信息,必须经过用户的明示同意并且符合法律法规及监管部门的规定。

- 1月22日,信标委就《信息安全技术 区块链信息服务安全规范》、《信息安全技术 公共域名服务系统安全要求》、《信息安全技术 信息安全事件分类分级指南》、《信息安全技术 安全技术 信息安全管理体系指南》4项国家标准面向社会公开征求意见。意见反馈截止日期为2021年3月22日。

(<https://www.tc260.org.cn/front/postDetail.html?id=20210122204335>)

- 1月22日,网信办发布了新修订的《互联网用户公众账号信息服务管理规定》(“规定”)。旨在进一步加强互联网用户公众账号的依法监管,促进公众账号信息服务健康有序发展。规定共23条,包括公众账号信息服务平台信息内容和公众账号管理主体责任、公众账号生产运营者信息内容生产和公众账号运营管理主体责任、真实身份信息认证、分级分类管理、行业自律、社会监督及行政管理等条款。规定自2021年2月22日起施行。公众账号信息服务平台应当将公众账号和内容生产与账号运营管理规则、平台

公约、服务协议等向所在地省、自治区、直辖市网信部门备案，上线具有舆论属性或者社会动员能力的新技术新应用功能，应按照有关规定进行安全评估。公众账号生产运营者应建立选题策划、编辑制作、发布推广、互动评论等全过程信息内容安全审核机制，加强信息内容导向性、真实性、合法性审核，与第三方机构开展公众账号运营、内容供给等合作，应与第三方机构签订书面协议，明确第三方机构信息安全管理义务并督促履行。

(http://www.cac.gov.cn/2021-01/22/c_1612887880656609.htm)

简析：互联网时代，诸多企业都开立了互联网企业公众号，用于企业形象展示、宣传产品或服务。在以上规定施行后，企业作为公众号的运营者属于该规定定义的公众账号生产运营者，有必要比照该规定判断有无不合规之处，及时整改确保合规。作为公众账号信息服务平台的企业，也应对照该规定核查是否存在不合规之处。

- 1月26日，为进一步加强物联网安全标准化工作顶层设计，工信部组织制定了《物联网基础安全标准体系建设指南（征求意见稿）》（“征求意见稿”）并向社会公开征求意见。征求意见稿中规定了物联网基础安全标准体系以及标准体系项下关于总体安全要求、终端安全、网关安全、平台安全、安全管理的五大类标准。征求意见稿的制定旨在加强物联网安全标准顶层设计和方向引领，推动构建系统、科学、规范的物联网基础安全标准体系，指导物联网安全工作的有序开展，支撑经济社会数字化转型和高质量发展。

(https://www.miit.gov.cn/gzcy/yjzi/art/2021/art_de99ecee64884ecda932604c32631b76.html)

➤ 境外立法

◇ 欧盟

- 1月15日，欧洲数据保护委员会（EDPB）和欧洲数据保护监督员（EDPS）就欧盟委员会于2020年11月发布的标准合同条款草案（“SCCs草案”）通过了联合意见。SCCs草案既适用于个人数据向第三国传输，也适用于欧洲经济区内的控制者和处理者关系。

(https://edpb.europa.eu/news/news/2021/edpb-edps-adopt-joint-opinions-new-sets-sccs_en)

◇ 美国

- 1月19日，美国商务部发布《确保信息和通信技术及服务供应链安全》的最新规则（Securing the Information and Communications Technology and Services Supply Chain），旨在落实2019年5月15日特朗普政府第13873号总统令（《确保信息和通信技术及服务供应链安全的总统令》）中列明的相关要求，建立并完善“用于识别、评估和处理美国人与外国人之间涉及设计、开发、制造或提供信息和通信技术或服务的某些交易”的流程和程序。该规则计划于2021年3月22日生效。

(<https://www.federalregister.gov/documents/2021/01/19/2021-01234/securing-the-information-and-communications-technology-and-services-supply-chain>)

◇ 韩国

- 1月14日，韩国个人信息保护委员会于2021年1月向社会公众发布《个人信息保护法（修正案草案）》。修订内容包括完善与其他立法进行制度衔接、完善自律机制、明确移动图像信息处理设备的操作标准、明确数据跨境流动的多种渠道、建立隐私政策的审查机制等内容。

（<http://www.ctils.com/articles/917>）



执法聚焦

境内执法

- 12月29日,北京市第一中级人民法院出具裁定,驳回链家网某员工破坏计算机信息系统罪上诉案。原审法院认定,该员工利用其担任链家公司数据库管理员并掌握公司财务系统 root 权限的便利,登录公司财务系统服务器删除了财务数据及相关应用程序,致使公司财务系统无法登录。就上诉人提出的案件事实方面的怀疑,法院认为司法鉴定意见书和有关证据已证明员工案发当日(2018年6月4日14时至15时期间)在覆盖了通过IP地址为10.33.35.160远程以root身份登录链家服务器并通过执行rm、shred命令删除数据文件、擦除操作日志等的网络区域上班,而前述IP地址于6月4日14时17分被分配给MAC地址为EA-36-33-43-78-88、主机名为Yggdrasil的设备使用。经司法鉴定确认,该员工电脑的主机名为Yggdrasil,与登录服务器执行删除、擦除命令的电脑主机名一致;该员工电脑的MAC地址虽不是EA-36-33-43-78-88,但其电脑中安装有用于更改MAC地址的软件WiFiSpoofer,且在其电脑的相关文件中检索到多条与上述MAC地址相关的记录。综合案发后员工的表现,以及对具有类似权限人员所用电脑的鉴定结论等情况,能够确定该员工实施了删除链家公司财务系统服务器程序数据的行为。

(https://mp.weixin.qq.com/s/ygnK2OFakJn8uFlOG8Q_ag)

简析:从技术层面来说,动态分配IP地址,通过技术手段仍然可识别到具体的个人。MAC地址也可以识别到具体的主机和个人。从人力资源管理角度,向员工提供培训,提高安全意识和守法意识,一方面可保护企业系统、数据和财产的安全,另一方面也可预防员工“误入歧途”。

- 12月30日,据公安部发布的消息,2020年以来,全国公安机关深入推进“净网2020”专项行动,聚焦人民群众深恶痛绝的侵犯公民个人信息犯罪,持续开展集中打击行动,不断压缩侵犯公民个人信息活动空间。截至12月20日,全国共侦办侵犯公民个人信息刑事案件3100余起,抓获犯罪嫌疑人9700余名,有力震慑了侵犯公民个人信息犯罪分子嚣张气焰,有效维护了网络空间秩序和人民群众合法权益。

(<https://baijiahao.baidu.com/s?id=1687497929953724582&wfr=spider&for=pc>)

简析:“净网”行动持续进行,打击了不少侵犯公民个人信息犯罪。相信多部门开展的打击侵犯公民个人信息违法违规行为行动将从执法层面有力提升保护公民个人信息的意识。

- 1月5日,工信部网站公示了2020年“双随机一公开”检查结果。2020年,工信部网络安全管理局组织对部分电信和互联网企业、域名机构的网络安全防护工作情况、网络与信息安全责任落实情况、网络数据安全保护责任及管理措施落实情况、电话用户真实身份信息登记情况等开展随机抽查。此次抽查共发现49家电信和互联网企业、域名机构不同程度存在违规情况,均已向各企业反馈检查问题,明确检查整改要求并要求限期完成整改。

(https://www.miit.gov.cn/jgsj/waj/xyaqgl/art/2021/art_126d93c97aa74505b4d712031b477042.html)

简析：检查结果显示部分企业存在未及时更新定级备案信息、业务系统部分配置未满足相应等级通信网络安全防护标准有关要求或业务系统未开展符合性评测工作等问题，部分企业存在数据安全管理制度、技术保障措施不符合相关法律法规要求的问题。该检查围绕网络安全等级保护制度问题，尽管是对部分电信和互联网等领域企业开展，但突显出国家强化网络安全等级保护制度执法的趋势。对于广大企业来说，有必要比照网络安全等级保护制度相关要求，核查自身是否满足等级保护制度各方面要求（包括技术层面和管理制度层面）。

- 1月13日，工信部近日印发通知，部署开展工业互联网企业网络安全分类分级管理试点工作。初定天津、吉林、上海、江苏、浙江、安徽、福建、山东、河南、湖南、广东、广西、重庆、四川、新疆等15个省（区、市）开展试点。通过试点，将进一步完善工业互联网企业网络安全分类分级规则标准、定级流程以及工业互联网安全系列防护规范的科学性、有效性和可操作性，加快构建工业互联网企业网络安全分类分级管理制度；进一步落实试点企业网络安全主体责任，形成可复制可推广的工业互联网网络安全分类分级管理模式；总结一批工业互联网网络安全典型解决方案，选拔一批优秀示范企业、培育一批专业服务机构。

(https://www.miit.gov.cn/jgsj/waj/gzdt/art/2021/art_eb95e60794794fc29f768233e7d7739d.html)

简析：联网工业企业分级主要考虑企业所属行业网络安全影响程度、企业规模、企业应用工业互联网的程度、企业发生网络安全事件的影响程度等要素，根据所属行业网络安全影响程度由低到高分别划分为一类、二类和三类（属于三类行业的规模以上联网工业企业原则上为三级）。企业分级方面，在安全管理方面，分别从组织管理、安全防护、风险评估、应急管理方面对三级企业和二级企业提出了要求。

- 1月17日，据媒体报道，近日由浙江省杭州市下城区检察院提起的民法典实施后全国首例个人信息民事公益诉讼案件，杭州互联网法院通过网络开庭审理并当庭作出判决，支持检察机关的全部诉讼请求，判决孙某赔偿损失3.4万元，并在省级新闻媒体公开赔礼道歉，相关赔偿款项将专门用于个人信息保护或信息安全保护等公益事项。

(https://www.spp.gov.cn/zdgz/202101/t20210117_506683.shtml)

简析：个人信息主体提起个人信息保护类别的诉讼可能面临举证困难的困境。可以预见，未来会有更多此类公益诉讼。

- 1月19日，上海一中院对全国首例电商平台涉反通知义务网络侵权责任纠纷上诉案进行公开宣判。上海一中院认为，投诉方供货商因重大过失导致错误投诉，淘宝公司在证据审核过程中存有过错，导致未及时终止处罚，网店售卖投诉商品存有不当且未积极维权，亦存在一定过错，改判酌定网店损失20万元，供货商、淘宝公司和网店分别承担50%、30%和20%的责任，并判令淘宝公司限时恢复网店积分和保证金。

(https://mp.weixin.qq.com/s/85_XrFo_gZj732edSN6mg?scene=25#wechat_redirect)

简析: 电商平台为避免损失,可借鉴本案中法院的认定标准,优化处理申诉的流程,比如给予处罚的时间期限以及就网店的申诉材料要求和供应商的投诉材料要求采用标准相同的证据证明层次;同时,在双方均提供证据的情况下,根据证据的情况及时告知供货商应向有关部门投诉或者向人民法院起诉。

- 1月21日,据媒体报道,天津市第一中级人民法院召开新闻发布会,通报一起因买卖非法收集个人信息产品而引发的合同纠纷案件。该案中,当事人双方签订了买卖“未经个人信息主体同意即可获得手机MAC地址”产品的合同。法院认为,虽然手机MAC地址本身不能识别用户的身份,但与其他信息相结合,可以获取该手机用户的电话号码,因此,手机MAC地址属于法律规定的与其他信息结合识别自然人个人身份的信息。最终判决认定买卖非法收集个人信息产品的合同无效、并对生产商、经销商买卖非法收集公民个人信息的电子产品所取得的财产予以收缴。

(<https://baijiahao.baidu.com/s?id=1689556332686291023&wfr=spider&for=pc>)

简析: 本案为企业从个人信息保护角度评估运营的产品或服务是否涉及个人信息、涉及与其他信息结合识别自然人个人身份的信息敲响了警钟。

- 1月25日,上海市青浦区人民法院对用户诉爱奇艺侵犯隐私权一案进行了一审宣判,称平台可以查看和使用用户的个人信息,在此案中平台并未滥用优势地位,判决用户败诉。庭审之后,用户在其个人微博中表示,自己对此判决有异议,将会上诉。2020年6月,北京互联网法院对会员诉爱奇艺《庆余年》超前点播案进行宣判,一审爱奇艺败诉。2020年7月,原告认为,爱奇艺在庭审中拿出自己上百页观影记录,侵犯了自己的隐私,再次将爱奇艺告上法庭。

(<https://new.qq.com/rain/a/20210125A06FWF00>)

简析: 诉讼中披露的信息如属于个人隐私,根据《民事诉讼法》的规定,涉及个人隐私的证据应当保密,需要在法庭出示的,不得在公开开庭时出示。《最高人民法院关于人民法院在互联网公布裁判文书的规定》中提及,人民法院在互联网公布裁判文书时,应当删除下列信息:家事、人格权益等纠纷中涉及个人隐私的信息。前述规定已经对隐私予以保护与查明案件事实作了适度的平衡。

在个人信息保护的法律领域,我国法律法规尚未明确规定于诉讼中披露个人信息无需个人同意。从举证角度,当事人提交的证据需要具备合法性要求,本案突显的问题是一方合法掌握的包含个人信息的材料可否在针对个人信息主体的诉讼中作为证据提供。本案一审法院的判决已然表明了态度。期待本案未来推动个人信息保护法律法规在举证所涉个人信息/隐私方面进一步完善,明确诉讼、仲裁案件中为举证需要提供个人信息可否作为处理个人信息的合法基础。

➤ 境外执法

◇ 欧盟

- 1月8日,德国下萨克森州数据保护机构(LfD)依据GDPR对Notebooksbilliger.de AG处以1040万欧元的罚款。该公司在没有任何法律依据的情况下对员工进行了至少两年的视频监控。这些摄像头覆盖了工作场所、销售室、仓库和公共区域等。该公司主张安装

摄像头的目的是为了预防和调查刑事犯罪、监测仓库货物的流向。下萨克森州数据保护机构指出，为调查犯罪目的安装视频监控仅在对特定个人存有合理怀疑时才是合法的，且仅能在限定的时间段监测这些员工。然而，该公司的视频监控既不限于特定的时间，也未限于特定的员工；且在很多情况下，监控记录被保存了 60 天，大大超过了必要的时间。该 1040 万欧元的罚款是 LfD 根据 GDPR 开出的最高罚单。

（<https://lfd.niedersachsen.de/startseite/infothek/presseinformationen/lfd-niedersachsen-verhangt-bussgeld-uber-10-4-millionen-euro-gegen-notebooksbilliger-de-196019.html>）

- 1 月 19 日，根据 DLA Piper 发布的最新的年度报告显示，自 GDPR 生效以来，数据保护当局已对各种违规行为开出 2.725 亿欧元罚款。意大利开出了大约 6,930 万欧元的罚单，为欧盟最高。德国和法国分别以 6,910 万欧元和 5,440 万欧元的罚款总额位居第二和第三。该报告显示，在这段时间内，已经有超过 28.1 万份数据泄露通知被报告，其中德国发布的数量最多，达到 77,747 份。

（<https://www.dlapiper.com/en/uk/insights/publications/2021/01/dla-piper-gdpr-fines-and-data-breach-survey-2021/>）

✧ 美国

- 1 月 14 日，脸书（“Facebook”）在葡萄牙对两名葡萄牙国民提起诉讼，指控他们开发浏览器扩展程序从 Facebook 网站抓取用户数据。Facebook 执法与诉讼负责人表示，当用户访问 Facebook 时，这些扩展程序会根据预先设定的编程抓取用户的姓名、用户 ID、性别、感情状态、年龄段以及与其账户有关的其他信息。据悉，扩展程序由一家名为 Oink and Stuff 的软件公司开发。截至目前，扩展程序仍可在官方的 Chrome Web Store 上使用，并且总共安装了 54,000 多次。对此，Facebook 要求葡萄牙法院对 Oink and Stuff 公司发布永久禁令，并要求该公司删除其通过扩展程序获得的所有 Facebook 用户数据。

（<https://mp.weixin.qq.com/s/egImtgqvneNwUm6d0p86hw>）

行业新闻

境内新闻

- 12 月, 几十余名明星“健康宝”照片遭泄露, 被人在网上兜售照片。据报道, “健康宝”, 截至 11 月 1 日已覆盖北京市民和来京人员, 累积查询超过 17 亿次; 经有关人员实测发现, 在其健康宝的“他人核酸检测结果代查”功能中输入其他人的姓名和身份证号并点击“确定”, 即可显示其他人在健康宝中登记的人脸照片。“健康宝”的该代查功能系为照顾没有智能手机、不会使用智能手机的人群, 然而却被不法分子利用, 违法获取他人信息。

(<https://m.mp.oeeee.com/a/BAAFRD000020201228404874.html?layer=2&share=chat&isndappinstalled=0>)

- 1 月 5 日, 虾米音乐官方微博发布消息称, 由于业务发展上的调整, 虾米音乐服务将于 2 月 5 日 0 点停止服务。2021 年 1 月 5 日 10 点将停止该服务的账号注册、会员充值、虾币充值、专辑购买等服务, 开启用户个人资料与资产处理通道。对于用户信息, 虾米将根据国家法律法规及《虾米音乐隐私权政策》进行保存, 保存期限到期后将进行删除、注销或匿名化处理。

(https://www.weibo.com/xiamixiamixiami?refer_flag=1005055013_https://h5.xiami.com/app/xiami-frontend/xm-announcement/index/index.html)

- 1 月 6 日, 小红书 App 出现无法正常运行情况, 用户搜索后页面显示“没有找到相关内容”。也有部分用户表示自己的小红书 App 显示正常。随后小红书回应表示, 因第三方云服务供应商技术故障, 1 月 6 日早 7 点左右部分用户出现搜索、关注等功能无法使用的问题, 该问题已于 7:30 解决, 目前各项服务均可正常使用。

(<https://new.qq.com/omn/20210107/20210107A0BZ1600.html>)

境外新闻

◇ 欧盟

- 1 月 12 日, 欧洲药品管理局 (EMA) 宣布, 去年 12 月针对 EMA 的异常不明性质的网络攻击之后, 辉瑞生物科技公司有关 COVID-19 疫苗的数据被盗, 一些与 COVID-19 药品和属于第三方的疫苗有关的非法访问文件已经在互联网上泄露, 执法当局正在采取必要的行动。

(<https://www.computerweekly.com/news/252494741/Stolen-Pfizer-BioNTech-Covid-19-vaccine-data-leaked>)

- 1 月 14 日, 谷歌正式以 21 亿美元收购了可穿戴设备品牌 Fitbit。谷歌承诺, “我们将与全球监管机构合作, 采取保护消费者隐私期望的方式, 包括一系列有约束力的承诺, 确认 Fitbit 用户的健康数据不会被用于谷歌广告, 且这些数据将与其他谷歌广告数据分

开”。此外，欧盟还禁止谷歌限制其它品牌的智能穿戴设备的行为，以保证公平竞争。这些承诺有效期为 10 年，但欧盟可以选择延期。

(<https://www.verdict.co.uk/google-fitbit-acquisition-2/>)

✧ 美国

- 1 月 5 日，时任美国总统特朗普签署了一项行政命令，禁止与 8 款中国软件应用程序进行交易，旨在遏制中国软件应用程序对美国人构成的威胁。该命令认为，美国必须对中国软件应用程序开发商采取“积极行动”，以保护国家安全。该命令将于发布后 45 天内执行，它将禁止与“开发或控制”这些应用的人进行任何交易。上述 8 款应用软件包括：支付宝、扫描全能王 CamScanner、QQ 钱包、茄子快传 SHAREit、腾讯 QQ、VMate、微信支付、WPS Office 及其子公司的应用程序。

(<https://www.reuters.com/article/us-usa-china-tech-exclusive/exclusive-trump-signs-order-banning-transactions-with-eight-chinese-apps-including-alipay-idINKBN29A2PA>)

热点评述

互联网时代,企业和个人都活跃在互联网上,企业的互联网公众号发布产品或服务相关信息,起到宣传企业、建立维护企业形象的作用。作为员工的广大网名也在互联网、自媒体上“指点江山”,发表各种观点和看法。

实践中不乏企业员工状告企业侵犯隐私权的案例,其中不少案例均与企业实施内部用工管理权的调查方式、实施纪律性处罚的方式有关。当然,实践中亦不乏企业起诉员工侵犯名誉权的案例,其中不少与员工在社交媒体发布有关企业相关的消息或评论相关。近期引发热议的拼多多辞退匿名发帖员工的案例,涉及员工言论自由、企业调查员工违纪事实方式的合法性、企业调查违纪事实与员工个人信息权益、隐私权平衡等诸多问题。

本文就上述问题作出了解答,不仅论述了言论自由的边界问题,还就企业通过技术手段调查员工违纪事实、企业对员工实施纪律性处罚的方式等提出了合规建议。

从拼多多辞退匿名发帖员工看员工与用人单位使用社交媒体的法律风险

导语:

近期,拼多多辞退匿名发帖员工的消息引起关注。据媒体报道,拼多多前技术开发工程师在某职场社交平台匿名发帖,内容显示为“第二位拼多多猛士倒下了”,并配有一张办公楼外停放救护车的图片,定位则显示为拼多多办公点。该员工后被拼多多辞退。¹

拼多多方面于1月11日作出澄清,该员工被解约的真实原因不是因为其发布以上照片,该员工的言论(包括公司HR通过翻看其手机获悉其在匿名社区发帖等),为不实言论。公司方面通过该员工所发帖的某匿名社区公开页面外显ID,查询到其既往匿名发帖内容充斥不良“极端言论”,违反了公司员工手册的规定,因此与其解约。²

本文作者在下文中简要分析下述问题:(1)劳动者言论自由的边界问题;(2)用人单位涉互联网媒体使用方面的合规建议;用人单位所需关注的员工使用社交媒体风险;用人单位如何规制员工的社交媒体、互联网言论行为;调查员工违纪事实与员工隐私权、个人信息保护的平衡;用人单位行使人事处罚权与员工权益的平衡。

一、劳动者言论自由有其边界

言论自由是公民的一项基本权利。我国宪法第 35 条规定，中国公民有言论、出版、集会、结社、游行、示威的自由。但，自由和权利不是无限的，有其边界，否则不可能存在真正的自由和权利。劳动者的言论自由受到我国法律保护的其他权益的制约。

劳动者工作中与所在单位领导或同事存在分歧，通过群发邮件或通过微信发表贬损他人的言语，有没有问题？另，劳动者在下班后的言行，比如在互联网社交媒体等发布所在企业的的相关信息，是否属于其私事，企业不应干涉？下面列举几个案例。

案例：

案例一

上海浦东新区人民法院审结的一个劳动合同解除争议案例中，涉事劳动者作为派遣员工被派遣至某企业工作，由于对其主管给出的工作评级不满，该劳动者通过微信向主管发送威胁性言语，用工单位以其构成员工手册中规定的过错行为即“以各种方式威胁、骚扰、辱骂或人身攻击同事、驻派单位员工、与 xx 公司有业务往来的客户或供应商及其工作人员”退回劳务派遣单位，劳务派遣单位以其严重违纪为由，与其解除了劳动合同。法院最终认定系合法解除劳动关系。

案例二

北京市第三中级人民法院的一个劳动合同解除争议案例中，涉事劳动者认为其在公司受到了不公对待，在一些知名互联网及社交平台发表了几十篇与其所在单位相关的文章或录音，除存在部分客观事实的表述之外，亦存在大量具有贬损之意或攻击性词汇。

法院认为，根据其所在单位制定的员工手册，员工不得在公司以外使用互联网…或其他媒介发布泄漏该公司的信息或传播消息、提到该公司的信息，且该劳动者认可收到并知晓员工手册的规定，因此法院认定该劳动者在互联网及社交平台发布具有贬损含义或攻击性词汇的文章，严重违反了公司规章制度，驳回了该劳动者的全部诉请。

案例三

北京市东城区人民法院的一个劳动合同解除争议案例中，涉事劳动者在所在公司发出薪资减发通知后，在微信朋友圈发布了所在单位的激励计划讲话截图、公司内部薪资减发通知截图，被公司解除劳动关系。法院认为，该劳动者的行为虽有失妥当，但是公司并未证明涉事劳动者给公司造成了损失及后果；涉案劳动者及时删除了信息，消除了影响；用人单位处罚员工

需遵循比例原则（用人单位的处罚手段和劳动者给用人单位造成的损害之间要符合比例）。法院最终认定用人单位构成违法解除，但法院的如下观点值得关注。法院的观点归纳如下：

劳动者在发表涉及所在公司事务的言论时，不再仅仅属于自由处分私人事务，而是涉及到了他人的利益，劳动者在发布相关信息时应负有更高程度的注意义务。

劳动者除了负有提供劳动的主义务外，还负有维护劳动秩序的从义务，即忠实义务。劳动者有义务在可期待的范围内维护用人单位的商业利益……不论对外发布的信息是否属于商业秘密，作为一名员工均不应该将公司内部信息随意发布社交媒体。

简析：

本文作者还检索到了很多其他类似案例，比如劳动者认为自己遭受了不公待遇，向用人单位内其他部门领导群发邮件，或对公司内某些事务不满群发邮件，导致被用人单位解除，引发了劳动合同解除争议。

互联网已然渗透到我们日常生活以及工作的方方面面，非工作时间通过互联网发送消息、发布信息，如果涉及到所在用人单位的信息，已然不能将我们在互联网上的言行归结为私人事务。以上北京市东城区人民法院的判决中，法官的论述精彩，非常值得关注。

劳动者如果将企业有关信息随意发布在互联网或社交媒体中，如果用人单位有合法实施的内部制度明令禁止，随意发布该等信息本身就已构成违反内部规章制度或违纪行为，将受到处罚。至于该等行为是否达到用人单位可解除劳动关系的严重程度，还需根据比例原则，结合具体案情予以判定。

如果劳动者的以上行为，情节严重，构成侵害了所在用人单位的合法权益（如，名誉权），劳动者不仅面临劳动法方面的后果（受到内部处罚），还可能得向用人单位承担民事侵权责任（如，名誉权侵权责任）。

二、用人单位涉互联网媒体使用方面的合规建议

1. 用人单位所需关注的员工使用社交媒体风险

互联网已成为众多企业展示企业形象的舞台。一方面，企业需要关注、培训相关岗位员工了解企业自身的社交媒体账号或官网发布信息需符合的合规要求（如互联网内容治理、广告法方面的合规要求），避免信息发布触碰合规红线或侵害他人的合法权益，如他人

的知识产权、名誉权等；另一方面，企业还需特别关注、预防员工的互联网媒体账号发布信息导致侵害企业自身合法权益的情形：

（1）企业员工不慎发布的信息如果包含企业的商业秘密（如经营策略、企业财务信息、供应商名单、客户资料以及其他需要保密的信息等），可能影响或丧失企业在市场上享有的某些竞争优势。

（2）企业员工发布的信息如果泄漏了企业的客户信息，如果与客户的合同中含有相应保密条款，则可能构成合同违约。

（3）企业员工在网上发布的信息如果不当，或者发布诋毁、贬低企业自身的信息，可能给企业自身的形象、声誉带来负面影响，甚至导致企业的舆情危机，影响企业的正常经营。

2. 用人单位如何规制员工的社交媒体、互联网言论

如前文所述，员工作为自然人享有言论自由的权利，在人力资源场景下作为劳动合同一方的员工发表涉及用人单位的信息，就不再仅属于员工私事范畴，应尽到注意义务。为了规避可能产生的风险，用人单位可通过制定合理合法的规章制度，引导约束员工的社交媒体行为，从而保护用人单位自身的合法权益。用人单位的规章制度中可就下述问题作出规定：

- （1） 界定保密信息的范围，可以详细列举+概括条款方式确定，明确未经用人单位事先同意，保密信息不得通过任何方式披露或公开；
- （2） 员工未经用人单位同意，不得发布保密信息以外的特定信息（可根据具体情况列举详情，比如客户名称）；
- （3） 员工未经用人单位事先同意，不得发布贬损、诋毁或任何其他有损本企业形象、声誉的行为，包括不得在互联网、社交媒体发布该等信息。

就用人单位内部的沟通，可在规章制度中规定员工不得发送过激、威胁、恐吓性质的言语，维护公司正常的工作秩序；并对员工的申诉提供可操作的流程和路径。

此外，用人单位可就违反上述规定的行为根据比例原则设置相应的纪律性措施。

3. 调查员工违纪事实与员工隐私权、个人信息保护的平衡

回到文首的拼多多事件，拼多多方面澄清，公司方面通过该员工所发帖的某匿名社区公开页面外显 ID，查询到其既往匿名发帖内容。本事件中，公司方面是如何快速查询、定位到该员工之前的发帖内容，在网上引起了一些讨论。³ 而该事件中的发帖平台 1 月 10 日公开回应，在用户信息管理上，在严格遵循国家相关法律法规的前提下，平台不以任何形式向任何第三方提供发言区发帖用户信息，且对于个人信息进行极为严密和完备的安全保障。⁴

据报道，拼多多方面系根据内部同事反馈，“高度怀疑”是该员工，后经该员工本人承认，方获知了匿名背后的真实信息。⁵因此，如果该等信息属实，外显 ID 和个人的一一对应关系可能并非通过技术手段实现。

本文作者无意就拼多多事件进行评论。单从技术层面角度，有关报道中，有技术专家表示：“只要……网络管理员把网络里连接……（外部平台）服务器的设备统计出来，再使用这些设备特征去匹配自己的网络服务，那么就会很容易找到发帖人”⁶。作者此处简要探讨企业通过技术手段开展违纪调查时的注意事项：

由于通过技术手段监测或追踪员工使用公司网络、电子设施设备的情况，可能不可避免会涉及到处理员工的个人信息，如果员工使用公司网络、电子设施设备通讯，公司网络传输内容中存在包含员工隐私信息、个人信息的可能性。在我国强化个人隐私权、个人信息权益保护的趋势下，需要确立企业通过技术手段调查员工的合法基础。因此，为了开展这些调查、监测或追踪行动，需要事先在内部规章制度或有关合同中就员工使用 IT 设施、设备、系统确立规则，员工不得利用企业的 IT 设施、设备、系统从事危害企业权益的行为，为公司 IT 系统、设施设备安全目的，或为对员工涉嫌违纪的行为展开调查目的，企业可以监测、收集处理有关信息（以及收集处理信息的范围）。

此外，如果涉及使用爬虫技术收集员工在社交媒体发布的言论等信息，应注意不应突破其他平台的保护性措施，否则，根据具体情况，可能构成侵犯特定个人的个人信息权益/隐私权的风险，非法突破他人系统的还可能涉嫌构成某些计算机网络相关的犯罪行为。

（关于爬虫技术涉及的法律问题，参见作者的文章：《网络爬虫技术是洪水猛兽吗？——浅谈网络爬虫技术采集信息所涉相关法律问题》）

4. 用人单位行使人事处罚权与员工权益的平衡：能否通过互联网公开违纪行为与处罚结果

用人单位对员工采取纪律性措施，是企业行使用工自主权的一种表现形式。但，即便采取纪律性措施有其合法依据，仍不可忽视用人单位采取纪律性措施的方式是否合法，比如：是否能将违纪处罚信息发布于互联网媒体，如企业的官网或微信公众号？

实践中，有些用人单位在公司内网或在互联网媒体（如微信公众号）发布员工违纪处罚的通告等，导致用人单位被员工诉至法院，主张用人单位构成名誉权侵权。纵观本文作者检索到的部分用人单位败诉案例，用人单位的行为有一些共性：用人单位并非仅向员工送达处理决定，在一定范围内或者通过互联网媒体向社会披露了处理决定等信息，用人单位披露的信息中含有影响员工名誉的信息（比如，无法证明的违纪事实）或含有员工隐私信息。

根据《民法典》，自然人享有名誉权，任何组织或个人不得以侮辱、诽谤等方式侵害他人的名誉权。名誉是对民事主体的品德、声望、才能、信用等的社会评价。如果用人单位认定的违纪行为其实并不属实，在企业内网或公告栏或甚至于互联网公布该等违纪行为就可能导致员工的社会评价降低后果，由此触发员工提起的名誉权侵权诉讼。

此外，《民法典》规定自然人享有隐私权。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。其中，私密信息包含的范围非常广泛，任何私人不愿意公开的信息都可能构成私人的私密信息，只要这种隐匿不违反法律和社会公德，都构成受法律保护的隐私。⁷

因此，用人单位应谨慎评估是否公布员工所受纪律性处罚信息。出于个人信息保护目的，应避免公布员工个人信息（姓名、身份证号等）。在一定范围内公布员工纪律性处罚信息的，除非拟披露的违纪事实铁板钉钉，通常不建议披露详情，缺乏可靠性的违纪事实认定一方面可能导致劳动法角度被认定为违法的处罚，另一方面可能导致构成侵犯员工名誉权。此外，即便违纪事实确凿无疑，如果违纪事实中包含涉事员工的隐私等，也不应予以披露，否则将触发隐私权侵权风险。

结语

互联网时代，人们凭借智能手机或其他智能手持设备就能在因特网上自如地浏览网页，在网络上发布信息（文字、音频或视频），与他人单独或通过群组交流。互联网传播的快速性和广泛性，带来了人们言论自由与其他法律法规予以保护的权益之间的冲突，员工使用互联网

媒体发布信息导致的解除案件，以及用人单位发布违纪处罚信息侵害员工名誉权等权益就是该等冲突的一个缩影。还是那句话，权利不能没有边界。使用互联网、自媒体等时需要多几分慎重，言论客观公正，勿逞口舌之快，互联网才能更“清朗”，才能少些纷争和法律风险。

¹ <https://news.163.com/21/0111/21/G03FC6Q800019K82.html>

² https://weibo.com/u/5692605404?nick=%E6%8B%BC%E5%A4%9A%E5%A4%9A&noscript=1&is_all=1#_rnd1610853785866

³

https://mp.weixin.qq.com/s?src=11×tamp=1610788801&ver=2832&signature=v24WfRe6B0Tp2teymtK-kg*6Z3BoGTPxHMps3YdFhHeAXSpjqv7K0gQpfkaYT6ZkTQX4hwlyg0YLB6ImvopGiPm*4TWDN5kq*pWGXgP7myS5xDgYc8gtbcZdfzmhiSww&new=1

⁴ https://weibo.com/taoumaimai?is_all=1

⁵ https://mp.weixin.qq.com/s?src=11×tamp=1610803138&ver=2832&signature=0jkd-s2C2AezP7WT4KjdiYQs240bdUBXudSBumZmsQwXU68bxck*772djt4EjgReK*ObQBLB8s-qvSSoJU2ZUVy5g3AYYeMZFx1oTTYtaVWe7fg-GrCRNuKBD8aCJGMP&new=1

⁶ https://mp.weixin.qq.com/s?src=11×tamp=1610803138&ver=2832&signature=0jkd-s2C2AezP7WT4KjdiYQs240bdUBXudSBumZmsQwXU68bxck*772djt4EjgReK*ObQBLB8s-qvSSoJU2ZUVy5g3AYYeMZFx1oTTYtaVWe7fg-GrCRNuKBD8aCJGMP&new=1

⁷ 《中华人民共和国民法典人格权编理解与适用》，人民法院出版社，2020年7月第1版，第341-342页。