



大数据时代如何更好实现个人信息保护和利用

近年来,随着信息化、数字化的持续深入,尤其是人工智能的出现,个人信息权益保护老问题与新风险叠加;与此同时,数据作为新型生产要素,个人数据是其重要组成部分。习近平总书记多次就个人信息保护问题作出重要

指示,强调要加强数据安全和个人信息保护。在实践中,我们要理清个人信息保护与个人数据开发利用的关系,把握好二者之间的边界,加强与落实政府、企业的治理责任,同时提高安全意识,防范个人敏感信息的泄露。

个人信息权益保护与个人数据要素化并行不悖

□ 时建中

个人数据与非个人数据是数据的基本分类。数据是数字经济的关键生产要素,经过较长时间消费互联网的推动,个人数据已经成为我国数字经济的重要要素。目前,我国不断织密个人信息权益保护规则网,筑牢保障数据安全的防火墙,质效明显。然而,由于个人信息的敏感性和个人数据的特殊性,个人数据由信息载体向生产要素的转换机制尚不健全,更加充分地释放个人数据的要素价值还面临一系列障碍。

个人数据并不完全等同于个人信息。对于个人信息的内涵与外延,《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第四条给予了明确规定,“个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息”。而关于个人数据尚无明确的定义,我们可以结合《中华人民共和国数据安全法》(以下简称《数据安全法》)的相关规定予以认识和理解,该法第三条规定,“本法所称数据,是指任何以电子或者其他方式对信息的记录”。可见,所谓个人数据就是任何以电子或者其他方式对个人信息的记录,换言之,就是任何以电子或者其他方式对与已识别或者可识别的自然人有关的各种信息的记录。在数字化时代,我们所讨论的数据,特别是能够作为生产要素的数据仅指电子数据。这是因为,只有电子数据才能成为生产要素。因此,信息与数据的一般关系可以描述为:相对于信息,数据是记录载体;相对于数据,信息是被记录的内容。信息与数据,有着相互对应的关系。随着数据量的增加,在信息与数据相互对应的基础上,衍生出数据之间的相关性,构成了数据的独特价值,形成了对初始信息的超越。鉴于此,尽管数据是信息的记录载体,信息是被数据记录的内容,但是,数据并不完全等同于信息,个人数据并不完全等同于个人信息。

两法确立了保护与利用并重的立法目标,不可偏废。鉴于个人信息保护的

必要性和数据安全的重要性,我国分别制定了《个人信息保护法》和《数据安全法》。对这两部法律的理解和适用,切忌望文生义和断章取义。为此,有必要全面准确把握这两部法律的立法目标,以实现纲举目张,发挥其应有的法律效益。

立法目标是一部法律的出发点和落脚点,规定了一部法律的基本价值追求和意图实现的效果。《个人信息保护法》第一条规定,“为了保护个人信息权益,规范个人信息处理活动,促进个人信息合理利用,根据宪法,制定本法”。据此,“规范个人信息处理活动”既要“保护个人信息权益”,又要“促进个人信息合理利用”,不可偏废。《数据安全法》第一条规定,“为了规范数据处理活动,保障数据安全,促进数据开发利用,保护个人、组织的合法权益,维护国家主权、安全和发展利益,制定本法”。据此,“规范数据处理活动”既要“保障数据安全”,又要“促进数据开发利用”,还要“保护个人、组织的合法权益,维护国家主权、安全和发展利益”。可以将两法的目标概括为“保护与利用并重”:保护是利用的前提,利用是保护的延伸;保护是为了防止滥用,利用是防止浪费;保护是为了维护正当权益,利用是为了赋能发展。

深入解构数据的双重属性,准确把握个人信息与个人数据关系的演变。电子数据是现代信息通信技术的产物,承载信息是数据的初始功能。作为信息载体,信息与数据不可分离,保护个人信息就必须保护个人数据。随着数据化的范围、广度、深度的不断拓展,海量数据得以生成。借助不断进步的数智技术,蕴含在不同数据之间的相关性不断被挖掘,派生出新的增量信息。挖掘数据之间的相关性显性地表现为挖掘信息内容的相关性,而信息内容的相关性能够揭示不同事物间的内在联系,反映社会、市场普遍的运行规律,赋能经济发展、社会治理和政府管理的运用场景。没有数据之间相关性的发现和运用,数

据只能止步于信息载体。数据的生成、加工、使用逐渐内化到生产经营过程中,成为新型生产要素,才能兼具信息载体和生产要素的双重属性。作为初始信息载体的初始数据,在要素化的过程中,不断被加工,生成了衍生数据。信息与数据之间的关系呈现复杂化的状态和趋势。增量信息源于初始信息,但又超越初始信息;衍生数据源于初始数据,但又超越初始数据。承载增量信息的衍生数据,与承载初始信息的初始数据,不再同一,初始信息与衍生数据不一定具有内容与载体的关系,增量信息与初始数据之间也不必然具有内容与载体的直接关系。信息与数据之间的这种演变,同样适用于个人信息与个人数据。因此,在保护个人信息与促进个人数据开发利用之间,应该划定合理界限:保护个人信息需要适用的数据范围,应该以保护个人信息权益为必要,既不宜过度扩张也不宜过度限缩。

个人信息与个人数据的保护与利用,需要法治与技术共同发力。在数字化时代,个人的身份、行为以及参与的社会关系均已数据化。作为以调整社会关系为己任的法治,需要主动引入数据思维和方式,以适应不断数据化的新趋势。数据是现代数智技术的产物,包括个人数据和个人信息在内的数据治理和信息保护,必须借助数智技术。从这个意义上讲,数据和数智技术不仅是法治的调整对象,而且是法治的赋能工具。

从保护和利用个人信息与个人数据的角度,可以考虑进一步加快构建个人信息匿名化制度。根据《个人信息保护法》第四条规定,个人信息不包括匿名化处理后的信息,实质性地将“匿名化处理后的信息”排除在个人信息之外。这一条直接切断了数据作为载体与个人信息之间具体单一的对应关系,为数据作为要素进行相关性挖掘提供了充足的空间。然而,我国个人信息匿名化制度目前主要面临两大困境:一是法律笼统地规定匿名化应当以“无法识别、不可复原”为标准,其具体内涵仍然不清;

二是现有标准规范混淆了匿名化与相关概念。未来应当进一步深入个人信息匿名化制度的理论研究,明晰有效匿名化的内涵,总结针对统一场景统一适用、不同场景应势调整的匿名化标准,明确匿名化后再识别行为的法律责任,开展匿名化效果动态监测评估,根本消除对个人信息无法完全匿名化的质疑与担忧。

与此同时,应当激励运用可以提高保护个人信息和个人数据的新型技术。例如,隐私计算、区块链、数据脱敏、数据沙箱等技术令数据在不同主体间“可用不可见”“可见不可取”“可控可计量”成为可能。这保障了数据载体—信息内容—信息主体之间具体单一的对应关系在挖掘数据之间相关性的过程中不被发现、不被利用,为个人数据在不同行业、不同地区、不同机构之间流通利用提供了安全可靠的技术环境。因此,需要从制度层面建立激励机制,引入保护隐私的安全技术,不断提高个人信息和个人数据保护的技术能力,加强通用技术体系研究,拓展场景化应用示范,建立一系列配套的技术规范与测评规范。

综上所述,当个人数据作为信息载体时,保护信息内容所蕴含的个人信息权益是优先目标,保护数据安全是保护信息内容安全的应有之义。当个人数据作为生产要素时,促进个人数据流通利用是优先目标。两个“优先目标”虽不一致,但必须统一起来,安全是发展的前提,发展是安全的保障。明确个人信息权益保护的底线,有利于保障个人数据流通利用的有序和效率;推动个人数据要素化,充分释放个人数据的要素价值,不仅可以推动经济发展,而且可以倒逼技术(包括安全技术)进步,持续提升个人信息保护的能力和水平。

(作者系中国政法大学副校长、数据法治研究院院长)



随着互联网和智能设备的普及,我们的生活变得更加便利,但个人信息泄露的风险也随之增加。从身份盗窃到数据泄露,个人信息安全问题与每一个人息息相关,成为社会广泛关注的话题。

在哪些情况下个人信息会被泄露呢?从现实情况来看,个人信息泄露的常见情境主要有以下几种。一是不安全的网络连接。公共 Wi-Fi 虽然方便,但也存在巨大的安全隐患。由于公共 Wi-Fi 网络通常缺乏加密保护,黑客可以轻松截取用户在网络上的数据传输,从而获取敏感信息。尤其是在进行网购、网上银行等操作时,使用不安全的网络连接风险更大,不法分子可以通过中间人攻击,截取用户的银行账户信息和密码。二是移动应用程序的权限滥用。许多移动应用程序在安装时要求获取大量权限,如访问通讯录、地理位置、相机等。通过访问通讯录和图片库,应用可以提供更流畅和更具个性化的用户体验。例如,社交媒体应用可以建议添加用户的联系人作为好友,而照片编辑应用可以让用户直接编辑和分享存储在手机上的照片。通过对用户数据的分析,可以帮助应用改进服务并更好地满足用户的需求。但是,如果用户随意授予这些权限,也会有应用程序收集并滥用用户个人信息的风险,带来隐私和安全方面的威胁。即便是正规应用程序,也可能因为漏洞或恶意代码而导致信息泄露。三是社交媒体的不当使用。社交媒体的广泛使用使得人们更容易无意中泄露个人信息。用户在社交平台上分享的照片、位置、日常动态等,都会成为潜在的安全隐患。不法分子可以通过分析这些公开信息,获取用户的生活习惯、家庭状况等,从而进行精准的诈骗活动。例如,在社交媒体上发布的家庭度假照片,可能会暴露家庭成员的具体行踪。四是网络钓鱼和欺诈。网络钓鱼是个人信息泄露的主要途径之一。攻击者通常通过伪装成合法机构,如银行、政府部门或知名企业,发送看似正常的电子邮件或消息,诱导受害者点击链接或下载附件,从而获取其敏感信息。钓鱼网站和虚假页面也是常见的手段,用户一旦输入信息,便会被不法分子窃取。例如,假冒银行的网站页面,要求用户输入账号和密码,用户一旦上当,这些敏感信息就会被盗用。

随着信息技术的进一步发展和应用,个人信息安全面临的挑战更加复杂艰巨,需要政府部门、有关企业和个人共同努力,共同构建一个更加安全的数字环境,保护我们的隐私和权益。政府部门应当制定和执行严格的个人信息保护法规,确保信息的合法使用并对违规行为进行严厉处罚。还需建立专门的监督机构,定期检查企业的信息保护措施,发布安全指引和最佳实践,确保信息安全的法律法规能够有效落地。日常应避免使用公共 Wi-Fi 进行敏感操作,如网购等。如果必须使用公共 Wi-Fi,则尽量不传输敏感信息,特别是涉及个人账户、密码及隐私方面的信息,以确保数据传输的安全性。二是小心应用程序权限。在安装移动应用程序时,要仔细阅读权限请求,对于那些不必要的权限应拒绝授予。定期检查已安装应用的权限设置,撤销不必要的权限,减少信息泄露的风险。例如,只授予应用程序执行其主要功能所需的最低权限,而不是授予所有请求的权限。三是谨慎分享个人信息。在社交媒体上分享个人信息时要保持谨慎,不要公开电话号码、家庭住址等敏感信息。定期检查隐私设置,确保只有信任的人可以看到你的个人资料和动态。例如,在分享旅行计划时,让亲密的朋友和家人知道即可,而不是向所有人公开。四是提高安全意识。首先,我们需要学会识别网络钓鱼和欺诈行为。不要随意点击陌生邮件中的链接或下载附件,尤其是那些要

公众如何认识和防范个人信息泄露

□ 王永建

求提供敏感信息的邮件。访问网站时,要仔细核对网址,确保其合法性和安全性。例如,银行和政府机构通常不会通过电子邮件要求提供敏感信息,因此对于这类要求要特别警惕。五是定期监测个人信息。定期查看银行账单、信用报告等,监测是否有异常交易或未经授权的活动。如果发现可疑情况,应及时与相关机构联系,采取必要措施。例如,通过定期查看信用报告,可以及时发现并处理身份盗窃的情况。

随着信息技术的进一步发展和应用,个人信息安全面临的挑战更加复杂艰巨,需要政府部门、有关企业和个人共同努力,共同构建一个更加安全的数字环境,保护我们的隐私和权益。政府部门应当制定和执行严格的个人信息保护法规,确保信息的合法使用并对违规行为进行严厉处罚。还需建立专门的监督机构,定期检查企业的信息保护措施,发布安全指引和最佳实践,确保信息安全的法律法规能够有效落地。日常应避免使用公共 Wi-Fi 进行敏感操作,如网购等。如果必须使用公共 Wi-Fi,则尽量不传输敏感信息,特别是涉及个人账户、密码及隐私方面的信息,以确保数据传输的安全性。二是小心应用程序权限。在安装移动应用程序时,要仔细阅读权限请求,对于那些不必要的权限应拒绝授予。定期检查已安装应用的权限设置,撤销不必要的权限,减少信息泄露的风险。例如,只授予应用程序执行其主要功能所需的最低权限,而不是授予所有请求的权限。三是谨慎分享个人信息。在社交媒体上分享个人信息时要保持谨慎,不要公开电话号码、家庭住址等敏感信息。定期检查隐私设置,确保只有信任的人可以看到你的个人资料和动态。例如,在分享旅行计划时,让亲密的朋友和家人知道即可,而不是向所有人公开。四是提高安全意识。首先,我们需要学会识别网络钓鱼和欺诈行为。不要随意点击陌生邮件中的链接或下载附件,尤其是那些要

个人信息保护与数据有序使用要平衡发展

□ 党燕妮

个人信息保护本是个老生常谈的问题,但随着大数据、区块链、大模型等技术的不断革新,个人隐私泄露、数据滥用等现象日益加剧,更加难以防范,成了挥之不去的“新病”。这就意味着,个人信息保护不能用旧药方治新病,需与时俱进、平衡发展。

数字经济时代,个人信息是一座数据富矿,具有巨大的社会与经济价值,充满了无限的创新空间和可增值性,也因此成为信息“黑产”市场中的“唐僧肉”。如何平衡好个人信息使用过程中数据保护与数据利用之间的关系?是以安全名义将个人信息“深藏闺中”,还是适度包容、鼓励“变数为宝”,成为数字治理相关法规政策制定与执行的难点与挑战。一段时间以来,对于个人信息数据的使用与管理,我国总体上采取了鼓励创新、审慎监管的发展模式,为激活数据红利创造了充足的空间。事实上,我国大量与大数据相关的技术和商业模式等的蓬勃发展也正是得益于较为宽松的制度环境。但这并不意味着对个人信息的轻视,“大数据比你还懂你自己”,背后隐藏的是个人隐私泄露的风

险和人们对个人信息控制权的丧失,而尊重公民对个人信息使用的选择权与知情权,是构建数字信任的关键。

近年来,随着个人信息保护相关法律法规的不断完善,尤其是2021年《中华人民共和国个人信息保护法》的施行,围绕个人信息已经形成了民事责任、行政责任与刑事责任三重责任保护机制,个人信息保护基本实现了有法可依。但也要注意,随着数据价值的不断释放,个人信息的社会性和公共性日益增强,个人信息保护不仅关涉个人利益,更关涉社会整体利益。比如,近年来因个人信息泄露、违法采集、使用而引发的“大数据杀熟”、算法歧视甚至网络诈骗、电信骚扰等乱象频发。同时,个人信息侵害行为事前防范难、事中制止难、事后取证难的特点,造成个体维权难度大、成本高、意愿低,为相关企业留下了较大的寻租空间,造成了“劣币驱逐良币”的市场氛围,严重影响到企业之间的正当、良性竞争。又如,在数字政府建设层面,随着政府间数据共享范围的不断扩大,跨领域、跨部门、跨层级的涉及个人信息

的碎片数据经过汇聚共享、融合关联和深度挖掘,可以迅速形成对个体行为轨迹、个性需求、价值认知等方面的全方位立体画像,这类数据一旦泄露或被非法利用,将严重损害个人与公共利益,甚至对国家安全带来较大风险。

由此可见,个人信息保护,究其本源是如何应对大数据时代科技发展对人的基本权利和自由所造成的挑战与侵害。而个人信息保护的复杂性,在于海量的个人数据之上,汇集了商业、社会、政治等多个方面以及个人、企业、政府等多方主体的不同类型与性质的权益。与此同时,个人信息保护又高度依赖于具体场景中个人与信息收集者、处理者之间的不同关系,不同情境下法律赋予的个人权利或个人信息流通规则也存在很大差异,如政府部门出于公共利益对于个人信息收集的原则就与日常商业场景中的平台网站收集消费者信息原则完全不同。这就要求个人信息保护需要政府、企业、个人之间协同发力,在个人权益有效保护、数字经济健康发展以及政府治理效能提升之间寻找最

佳的制度与政策平衡点。首先,政府需明确框定个人信息数据采集、处理、使用的边界。在此基础上,尽可能类型化不同场景中存在的问题,解决具体情境中存在的个人信息保护制度供给不足的问题,在立法与执法的交互过程中,不断推动制度的完善与更新。其次,企业应增强合规意识,切实承担起对其收集到的个人信息的安全保管责任,使用个人信息应当严格遵循合法、正当、必要原则,尊重消费者的知情权与同意权,依法依规做好个人信息的“守门人”。最后,个人也要不断提高信息保护意识,拧紧信息泄露的“安全阀”,筑牢信息提供“安全网”,守好个人信息安全的“城堡”。

总之,良好的个人信息保护是数据共享的前提,只有各方共同努力,做好个人信息保护与有序使用之间的平衡,才是数字经济健康发展的长远之计。



(作者系国家互联网应急中心研究员)