金融领域数据滥用让个人信息近乎“裸奔”

月色灯山满帝都,香车宝盖隘通衢……

月色灯山下,盛唐长安城内人流如潮。为找出细作,治安官吏在庞大档案中迅速找到关键信息,选派衙差破案。这是电视剧《长安十二时辰》中的场景,展现了“大案牍术”在唐代上元节的运用。这种基于档案数据推进事务处理的方法,使得破案、寻人等工作变得高效。电视剧中,“大案牍术”以推演嫌疑人户籍、行为信息为核心,成为剧情发展的推动力。《长安十二时辰》的成功让“大案牍术”这一大数据理念为公众所熟知。

利剑双刃,自古至今。技术进步在发挥向善一面的同时,破坏力也同样巨大。

小王是一名普通的上班族,平时会使用信用卡在网上购物。有一天,他突然接到了一个陌生电话,声称自己是某金融公司的工作人员,告知小王有一笔逾期债务需要立即清偿,否则将采取法律手段追讨。对方提供了小王的详细个人信息,包括最近的消费记录、家庭地址等,让他感到十分恐慌。后来,小王报警求助。经过警方的调查,发现他的个人信息被不法分子通过黑市渠道获取,用于实施暴力催收。

在当下,数据资源这座“宝矿”迅速成为商业化拓展的利剑,尤以金融业最明显。不同于线下传统模式,互联网金融依赖大数据进行创新。无论信用评估、欺诈检测等风险管理,还是精准营销、细分客群等个性化服务,通过分析海量数据,金融机构能更好地了解客户需求,提升风险管理能力,优化业务流程,提高运营效率。

不过,多位受访人士对记者表示,受企业利益驱动、组织道德缺失、数据治理不完善和用户意识不足等影响,大数据在互联网金融领域被滥用,甚至损害消费者权益的情形日渐增多,亟须更为有效地防范和治理。

在当今数字化时代,个人信息保护至关重要。个人信息的泄露可能导致身份盗窃、金融欺诈等严重后果,因此,每个人都应该采取必要的措施来保护自己的隐私。随着科技的发展和社会对个人隐私保护的关注不断增加,国家法律法规也在不断完善。个人信息保护不仅是一项技术问题,更是一项重要的社会责任。通过采取适当的措施,并密切关注相关法律法规的完善,公民可以更好地保护自己的隐私权,确保个人信息的安全和保密。

北京市高级人民法院发布的《侵犯公民个人信息犯罪审判白皮书》,针对近五年来全市法院审结的侵犯公民个人信息罪案件作出调研统计和实证分析。

有**超1/3**的涉案信息与公民人身安全、财产安全直接相关。

涉案信息要素中,手机号码、身份证件占比最大,合计达**77.3%**。

经初步统计,已结案件中,涉案信息**56.8%**被用于业务推销,**39.6%**被用于违法甚至犯罪活动。

多环节“走漏”:可查5分钟前通话记录?

“我们有手段可以查到借款人最近一次外卖订单,最快在5分钟前的通话记录。”一位华北地区长期负责银行外包催收业务的公司员工告诉记者。

在一份已经公布的侵犯公民个人信息二审刑事裁定书中,记者也看到了类似的情况。根据被告人表示,其通过在服务器里输入一个手机号码,查询各种外卖订单,包括美团、饿了么、蜂鸟配送等外卖里面的信息,获得收货地址,这样的一条信息可以卖出40元左右的价格。

在上述案件中,多名被告互相买卖户籍信息、开房信息、征信信息、机主信息等各类公民个人信息,后予以出售牟利。其中一人为银行信贷部主任,他利用工作便利查询上万条公民个人征信信息进行出售。

有监管人士告诉记者,信息泄露的主体一般是机构内部员工,或者一些有盈利压力的私营主体,比如常见的教育培训机构贩卖学生家长信息。

但是除了被动地泄露,也有“主动”将自己暴露在泄露危险之下的情况。

根据2022年最高人民检察院发布5件依法惩治侵犯公民个人信息犯罪典型案例之一,王某和李某成立某信息咨询有限公司,该公司2015年7月成立后,最初主要是网络商业推广,后公司出现亏损。正如前述监管人士所言,王某和李某便决定出售公民信息牟利。

2018年1月至2019年6月,王某与李某二人前后雇佣五十余人,通过在网上刊登贷款广告、在公司的“点有钱”微信公众号设置贷款广告链接,吸引有贷款需求的人填写“姓名、手机号、有无本地社保和公积金、有无负债、房产和车辆持有状况、工资收入、有无保险、征信情况、借款需求、还款周期”等信息。

获取上述信息后,王某和李某指使员工将上述信息上传到公司开发的“点有钱”APP,再通过在微信群搜集、在“点有钱”微信公众号发放广告,获取银行、金融公司信贷员的姓名和手机号。

通过与信贷员联系,吸引他们在APP注册充值。信贷员充值后,王某和李某等人在未经信息权利人同意的情况下,将信息以每条30元至150元的价格出售给信贷员。通过出售上述信息,王某和李某等人违法所得共计450余万元。

2019年6月,公安机关立案侦查,将王某、李某等人抓获,从网站后台提取到公民个人信息共计31万余条。

非法“爬取”:一个用户的信息不到0.5元

大数据是指无法用常规软件工具捕捉、管理和处理的海量、高增长率和多样化的数据集合,它需要新处理模式以增强决策力、洞察力和流程优化能力。通俗来说,大数据就是计算机和互联网从现实生活中获取并转化为数字数据的集合。

而大数据面前,一个人可谓“无所遁形”。

在互联网金融领域,有一种细致的分工叫做大数据风控公司。其通过大数据这类技术帮助银行、持牌消费金融公司等机构获客和进行风险控制,而这也恰恰是信息泄露的重灾区。

行业竞争激烈,有些大数据风控公司为了在市场中占据优势,从经济动机出发,不惜一切代价使用不正当甚至违法的手段收集和利用用户数据。

“你能想象到你的通话记录、社保、公积金等各类数据,在这些公司为小额贷款机构输出风控的时候值多少钱吗?”西北地区一家网络小额贷款公司负责人反问记者。

“答案是一个用户的以上所有信息一共不到五毛钱,如果长期签订技术服务合同,使用他们的数据平台获取数据和分析数据,一年都用不了五位数(服务费用)。”前述负责人道。

“年初我注册了几家网贷平台但是没有贷款,5月份的时候我想申请银行的经营贷就不行了。后来有做大数据的朋友告诉我才知道,这种行为会被一家或者多家网贷APP在后台监控、窃取并向外发送,最后制作成提供给放款机构的标准化风控产品。也许我已经被标记为‘疑似资金紧张’了。”用户小王自嘲道。

不仅如此,记者以资金方(即放款机构)工作人员的身份曾从一家号称做云服务的大数据风控服务商处,尝试了解其能提供的具体数据类型。在获取的风控数据维度文件中显示,不单是网贷公司注册信息,就连注册的时间点也是风控的“有用信息”,比如用户究竟是在深夜、凌晨,抑或白天进行的贷款申请,都能够获取。

仔细想想不难明白,这些大数据风控公司并无自身场景平台(电商、外卖、出行等),如果不是获取了合法的渠道授权,那么合规性必然堪忧。

2020年,一家杭州大数据风控公司的判决书,揭开了网贷产业风控的神秘面纱。

根据裁判文书网信息,该大数据风控公司主要与小型银行机构以及非银网络贷款公司合作,为放款机构以及网贷平台提供需要贷款的用户的个人信息及多维度信用数据。

具体方式是,将该公司开发的前端插件嵌入上述网贷平台APP中,在贷款用户使用网贷平台APP借款时,用户需要在前端插件上输入自己的通信运营商、社保、公积金、淘宝、京东、学信网、征信中心等网站的账号及密码才能完成审核。

经过贷款用户授权,大数据风控公司的爬虫程序代替贷款用户登录上述网站,进入其个人账户,利用各类爬虫技术,爬取(复制)上述企事业单位网站上贷款用户本人账户内的通话记录、社保、公积金等各类数据,并按与用户的约定提供给网贷平台用于判断用户的资信情况,并从网贷平台获取每笔0.1元至0.3元不等的费用。

虽然该大数据公司在提供给用户的协议中表示,不会保存用户账号密码,仅在用户每次单独授权的情况下采集信息。但事实恰恰相反,该公司未经用户许可仍采用技术手段,长期在自己租用的互联网公司云服务器上保存用户各类账号和密码。在整个过程中,该公司有相对应人员负责编写具有保存用户账户密码功能的网关程序(即一种负责将外部流量路由到集群中相应服务的资源)。

截至案发时,相关部门对公司租用的服务器进行勘验检查,发现以明文形式非法保存的个人贷款用户各类账号和密码条数多达2100万余条。

不过,值得庆幸的是,其中大部分账号密码无法二次使用,仅有邮箱等部分账号密码未经用户授权被二次使用。最终,法院生效判决认为,该公司以其他方法非法获取公民个人信息,情节特别严重,构成侵犯公民个人信息罪。

“合规”获得:扫码领鸡蛋背后的风险

“我们的风控数据都是合法获得的。”一家银行机构的高管对记者强调。该银行在近年迅速扩大个人贷款业务规模,短短10年间,作为城商行,其个人消费贷已经达到千亿元规模。

“不可否认的是,金融科技发展以后,客户信息的对称性、可获得性以及便捷性都达到了极高的水平,大数据的规模化运用,是消费贷崛起的基础,相当于地基。”上述银行高管表示。

该银行高管表示,原本的风控手段简单,但是获得的数据单一,依赖用户在银行的信用记录和历史数据综合评估。但是大数据可以通过分析用户的互联网行为、消费记录、社交媒体活动等非传统数据源,对用户进行更加全面和精确的信用评估,帮助金融机构降低贷款风险,提高信用评估的准确性。

“学历身份可以看到用户是本科生还是研究生,如果学历程度达到博士,某种程度上认为该用户属于社会精英。从‘985’‘211’学校毕业的人,其逾期风险也可能会小一点。”前述银行高管说道。

那么,这种维度的数据获得如何确保合法性?

“你肯定见过银行铺设在小区或者高校线下扫码领取鸡蛋的摊位,或者一些开通某项服务送米面粮油的活动。包括银行机构与物业合作在小区业主物业群里发送的端午、中秋活动链接,只要业主通过分享在群里的链接进入活动页面,就会有一个对其基本的判断,进一步通过与物业合作,了解物业费缴纳的情况。就像从前很多银行与通信运营商合作一样,了解每个月用户的话费缴纳情况。”该银行高管进一步介绍道,大数据维度并不止步于网购记录、打车记录,用户在大众点评以及社交媒体上发布的信息,都可以用来勾画用户画像,所以消费贷的发展离不开大数据。

该银行高管强调:“在合规性方面,我们肯定会做‘脱敏’(即对某些敏感信息通过脱敏规则进行数据的变形,实现敏感隐私数据的可靠保护)。我们发去消息的时候是看不见客户相关情况的,只有客户主动申请,扫码注册授权后我们才能看到是哪个群分享链接进来的客户。”

谈及如此丰富的数据维度是如何在消费贷上下游产业链(泛指银行、消费金融公司、小贷以及相关科技公司)流通过程中确保合规性时,大成上海办公室合伙人彭凯律师表示,除了基本的信用类数据外,还有个人填写提交的信息(其中还包括个人的近亲属的信息)、消费类数据、个人偏好类数据、个人使用线上渠道(比如APP、小程序)时产生或收集的日志信息/设备信息/地理位置等,都属于非常丰富的数据维度。这些数据的流通过程实际上是数据交互的过程,不同的数据交互模式需要履行不同的合规义务,比如告知并取得用户授权,与受托方签署数据委托处理协议,开展个人信息保护影响评估(PIA)等。

彭凯认为,当前法律框架内的保护手段主要是规定个人信息处理者的义务,以及赋予个人信息主体权利,相关法定义务包括但不限于:处理个人信息前的告知和获取同意,制定内部管理制度和操作规程,采取相应的加密、去标识化等安全技术措施,定期对从业人员进行安全教育和培训,制定并组织实施个人信息安全事件应急预案,响应个人信息主体的权利请求等。同时,法律也赋予了个人信息主体知情、决定、查阅、复制、更正、删除、要求解释说明等权利,个人信息主体可随时行使这些法定权利,以保护其个人合法权益。

数据治理:宜多方共同合作堵漏

在彭凯看来,当前互联网金融领域的数据滥用问题,集中体现在个人信息的泄露和非法使用上。具体而言:首先,互联网金融领域中,金融营销和催收都是违法违规使用个人信息的重灾区,比如在委外催收环节,金融机构为了催收,可能违背必要原则向催收公司提供超范围的、不必要的客户个人信息,催收公司也会为了完成相应的指标,超出合理目的非法使用客户的个人信息。其次,金融机构的系统庞大而复杂,系统本身漏洞、权限管控不到位、修复不及时等安全隐患都可能导致信息泄露等安全事件的发生。另外,金融机构还会涉及与较多第三方之间的数据交互,包括系统的技术供应商、催收公司、营销合作的外包方等,数据交互的过程必然涉及数据的传输,对第三方管控不到位同样可能导致个人信息的泄露或非法使用。

事实上,当前暴露的数据安全问题已经得到了有关部门高度关注。

2021年11月1日,《个人信息保护法》正式施行。在信息化时代,个人信息保护已成为广大人民群众最关心、最直接、最现实的利益问题之一。《个人信息保护法》坚持和贯彻以人民为中心的法治理念,牢牢把握保护人民群众个人信息权益的立法定位,聚焦个人信息保护领域的突出问题和人民群众的重大关切。

对于金融机构应该如何切实履行保护用户信息的责任,彭凯介绍道,根据中国人民银行公布的金融消费者权益保护典型案例,“某银行分行的员工利用职务便利,在未经授权审批且没有合法、正当事由的情况下,通过银行主要业务系统私自查询、记录客户个人信息并将相关信息对外贩卖,事后该银行分行亦未及时向当地金融监管部门报告”,彭凯表示,通过该案例可以看出,金融机构不仅要在事前对业务系统进行严格的权限管控,重视对从业人员的安全教育培训,以及制定相应的安全事件应急预案等以防范个人信息被滥用的风险,还要在事后采取相应措施减小安全事件造成的损害或影响,比如及时启动应急预案,及时向监管部门报告等。

他将问题一分为二来看待:“对机构而言,需要持续关注数据保护相关法律法规的修订,同时也要了解新兴技术的发展及其相关的监管动态,结合自身业务适时调整内部合规政策。从消费者角度来看,技术的发展固然可以提高数据传输和存储的安全性,但数据泄露或被滥用的风险并未消失,仍应树立重视个人信息安全的意识,积极了解和关注个人数据保护方面的知识,谨慎提供自己的个人信息。”

彭凯建议,数据合规工作是持续开展、持续改进的过程,一般还要结合机构所处行业、自身现状来确定相应的改进措施。但有些基础工作确实是不可或缺的,比如完善内部制度和操作规程,机构内部需要有相应的制度规则,保证员工依规则处理数据,也通过制度或者规则来约束第三方合规开展数据处理活动;再比如机构需重视员工数据保护意识的培养和提升,因为实际业务开展过程中,通常是员工在操作系统或者处理数据,因此定期对员工进行安全教育和培训也十分必要。当然,具体合规工作开展中,适当借助外部专业机构的力量也是很好的选择。

“从很多金融机构每年公布的ESG(环境、社会和公司治理)报告中也可以看出,现在机构在数据安全和个人信息保护方面也在不断完善,以提高机构数据保护的整体水平。比如根据中国建设银行公布的相关报告,其在管理架构、制度规范、培训教育、第三方管控、内外部安全审计等多个方面都开展了合规工作。这也说明数据安全和数据保护工作并非一蹴而就,而是在持续进行、持续改进的。”彭凯说道。

对于数据保护未来的展望,彭凯表示随着技术的不断更新迭代,未来可能会出现更加安全和高效的数据传输和存储方法,多方计算、同态加密等新技术已经在开展这方面的探索和实践。但需要注意的是,新技术的出现可以在一定程度解决安全问题,但可能并不能解决合规问题,法律要求的单独同意、告知、PIA等合规问题并不会因为技术升级而被简化。

据《中国经营报》 作者:郑瑜