非法获取公民个人信息事件频发 谁来保护我们的网络安全?

上海已启动大数据地方立法

□法治报记者 王川

央视 3·15 晚会曝光了企业利用“探针盒子”非法获取海量公民个人敏感信息的问题，将网络信息数据安全再次推到全民关注的高度。

其实，媒体曝光的仅仅是冰山一角。随着互联网，尤其是物联网的发展，信息传输和共享变得更加简单，一方面方便了人们的生活，为科技发展提供了动力，但是也必须看到，数据信息发展背后存在的巨大安全隐患。

幸运的是，经信委等相关部门已经开始着手启动大数据立法的地方准备，也有一些政协委员为网络信息安全建设建言献策、奔走努力，希望通过建立“中国（上海）信息安全谷”的方式，推动上海乃至全国的信息安全建设。

3·15 晚会曝光小小探针盒子 暗中获取用户海量私密信息

今年央视 3·15 晚会曝光的一系列企业中，上海一家公司“榜上有名”。这家名为上海智子信息科技股份有限公司的企业，主要以机器人寻呼系统拨打骚扰电话。据央视报道，该公司总裁朱建秋称，一个机器人一天能打 5000 个电话。

那么，机器人所拨打的号码是从哪里来的？据了解，这些号码的来源，藏在小小的“探针盒子”里。当用户手机无线局域网处于打开状态时，会向周围发出寻找无线网络的信号，探针盒子发现这个信号后，就能迅速识别出用户手机的 MAC 地址，转换成 IMEI 号，再转换成手机号码。

一些公司将这种小盒子放在商场、超市、便利店、写字楼等地，在用户毫不知情的情况下，搜集个人信息，甚至包括婚姻、教育程度、收入等个人敏感隐私信息。

一家名为萨摩耶互联网金融服务有限公司的负责人告诉央视记者，他们和店面合作，一个月只花几百元。一家商场 11 个门，装了 11 个探针盒子。这些小盒子就安放在天花板的中空位置。

那么，这些盒子背后如此海量的数据又是从哪里来的呢?从业者告诉央视记者,这些大数据，主要来源于用户手机上所安装的一些软件。

璧合科技股份有限公司谭经理称，现在我们在安装软件的时候，第一步会需要我们填一个用户服务条例。安装这个软件，必须要点击同意后才能安装。安装好了之后，现在一般软件会要求给它开权限，是否允许访问你的通讯录、手机文件夹，访问你的电话、短信等。你点击允许之后，才能使用这个软件。然后在你使用软件时产生的用户数据，就可以用作商业营销用途。

为了能正常使用APP，用户只能同意被获取个人号码等信息，然而在用户不知情的情况下，这些个人信息却变成了一些企业的牟利工具，被房地产、贷款、教育培训等第三方公司，用作拨打骚扰电话等商业营销用途。

这些漏洞看似都只能盗取一些信息碎片，但经过大数据精准匹配，消费者的个人信息就会暴露无遗。

物联网时代“万物互联” 数据安全风险更加凸显

近年来，像上述案件这样的“个人信息泄露”事件并不少见，因涉及人数众多、涉及信息敏感，每次都在社会上引起极大影响。

在产业数字化转型、数据驱动的互联网时代，大数据、人工智能、云计算等新技术深度发展，5G 物联网通信模块、智能软硬件等应用广泛拓展，虽然给社会发展和人们生活带来了极大助益，但各项技术应用背后的数据安全风险日益凸显，网络信息安全亟待加强。

今年 2 月 18 日，中国首个 5G 火车站在上海虹桥火车站启动建设，并计划于今年 9 月完成 5G 网络深度覆盖。据介绍，通过 5G 网络，一方面可以解决火车站大客流场景下旅客的高速上网、高清视频通话等需求，更重要的是未来可以利用 5G 赋能智慧火车站，提升火车站、铁路系统的管理效率，提升火车站运行和服务品质。

5G 火车站的启动建设，标志着上海已启动 5G 网络部署。未来上海还将在更多行业、更多领域实施 5G 应用示范工程，通过 5G 和各行各业的连接产生化学效应，加快生产活动向数字化、网络化、智能化方向演进升级。

但我们也必须注意到，在未来万物互联时代，愈发复杂的物联网系统将带来愈加突出的安全问题。以无人驾驶为例，特斯拉汽车在各种场合都可以接入 WiFi，还可以接入 3G/4G 网络。还将与交通灯、交通台，甚至是和其他车互通互联。一旦信息被泄露或被不法分子利用，意味着会有更多潜在的攻击点。

根据第 43 次《中国互联网络发展状况统计报告》显示，截至 2018 年 12 月，我国网民规模达 8.29 亿，全年新增网民 5653 万，互联网普及率为 59.6%，我国网民规模全球第一，构建安全可信的互联网环境刻不容缓。

快递公司系统遭入侵 6 万条面单信息被盗

其实央视 3·15 曝光的仅仅是非法获取公民个人信息的冰山一角。在诸多行业领域，公民的个人信息安全正遭受严峻考验。

去年 7 月，本市青浦区某快递公司 IT 部门工作人员就通过公司技术日志发现，该公司所属触屏官网自 2018 年 4 月以来被人利用系统漏洞侵入计算机服务器系统内，通过订单查询接口非法获取大量客户数据，至案发时已被非法获取 6 万余条客户信息。

报案后，警方通过技术手段锁定一名涉嫌侵犯公民个人信息的犯罪嫌疑人龚某。龚某在老家被抓获时，还未来得及将非法获取的客户信息卖出。很快，他便交代了一切。

原来，去年上半年，龚某在某网上聊天群里看到，有人在叫卖一款可以获取某快递公司客户数据信息的黑客软件。他听说贩卖公民个人信息可以赚到钱，于是便联系了对方，花费 500 元购买了这种软件。

龚某按照卖家的提示，先是用他人的身份信息注册了云服务器，又购买了一个新手机号，通过短信验证登录进去后，将这款黑客软件程序安装在云服务器上。在激活软件运行程序后，出现了一个滚动显示数据的窗口。不一会儿，便生成了一个内有多个文档的文件夹。龚某打开文档，发现里面全是该快递公司面单信息数据，包含快递订单号、产品名称、收件人姓名、联系方式、收货地址等。

短短三四个月，龚某通过这种方法非法获取数万条面单信息，并将盗取来的数据信息储存在云服务器中。警方调取龚某使用他人身份注册的云服务器镜像数据，经司法鉴定，去年 4 月至 7 月期间，龚某所使用的云服务器 IP 地址向该快递公司网站发起请求 200 万余次，非法获得快递运单信息 10 万余条，去除重复后得到记录数 6 万余条。在对这些数据分析发现，涉及该快递公司运单涉案文档 900 余个，共 1.56GB。

因涉嫌侵犯公民个人信息罪，龚某被青浦区人民检察院依法提起公诉。青浦区人民法院审理后，以侵犯公民个人信息罪判处被告人龚某有期徒刑 3 年，并处罚金 6000 元。

据本案承办检察官介绍，该类犯罪成本低但危害不容小觑，犯罪分子多将信息贩卖给电商、中介、网络黑市甚至诈骗集团，容易滋生信息骚扰、网络诈骗、敲诈勒索等下游违法犯罪活动，给公民人身和财产安全造成巨大隐患。

本市已启动大数据地方立法 建议创设“上海信息安全谷”

今年全国两会期间，有全国人大代表聚焦“网络信息和数据安全”，建议通过立法切实保护这些信息。

全国人大代表、上海市经信委主任陈鸣波指出，由于数据的合法合规流动使用标准缺乏，高应用价值的数据无法安全合法地获取和流通，同时一些不法分子通过网络爬虫、黑客攻击、非法交易等手段获取数据，不断侵害公民、企业、政府等社会各方的权利。而目前我国相应的基础性法律仅有《网络安全法》，其中涉及大数据的条款仅从“健全用户信息保护制度”出发，对个人信息的收集和使用作出规定，但对于海量公共数据的脱敏使用缺乏具体标准界定，对于违法违规的数据使用亦没有明确标准说明。相关部门公正执法难度非常大，个人对于侵权申诉的渠道也难以获得。

据了解，2018 年 9 月 11 日，中国消费者协会发布的《APP 个人信息泄露情况》中遇到过个人信息泄露情况的受访者占 85.2%。仅在 2018 年 9 月，就有企业被曝强制向用户调取通讯录等多项隐私权限；随后，某集团被曝有 5 亿条数据在“暗网”兜售……大数据立法亟待加快进程。

针对上述问题，陈鸣波在今年全国两会期间提交了议案，建议修改网络安全法，授权有关区域先行先试公共数据开放法制建设，为今后制定基础性法律奠定基础。同时，增加公共数据使用安全内容和法律责任内容，建立健全用户信息保护制度，对违法使用者予以相应的处罚，情节严重者追究刑事责任，营造公共数据开放利用的公平法治环境。

据陈鸣波透露，目前，上海正在抓紧研究公共数据开放管理地方性法规，已全面启动立法工作。

在今年上海两会期间，不少上海市政协委员也关注到了信息安全问题，其中市政协委员，中国电信集团号百信息服务有限公司党委书记、总经理李安民从行业发展角度提出建议。他认为，上海需要大力推进信息安全产业的发展，加强个人数据保护、可信身份标识保护、身份管理和验证系统等领域核心技术研发和应用推广。积极创造有利于技术创新的政策环境，突破核心技术，加快安全可信产品推广应用。在管理、技术、人才、资金等方面加大投入，加快构建关键信息基础设施安全防护体系。

同时，李安民认为，还应加强产业协同，多方谋划、多措并举预防和打击通信网络诈骗、侵害公民个人信息、网络黑客、侵犯知识产权等行为，并提议筹建设立“中国（上海）信息安全谷”，将之建设成为我国最大的信息安全产业发展、企业和人才集聚区，以此带动上海市信息安全产业化，并成为长三角地区乃至全国信息安全产业发展的引擎。