保护公民信息安全 中国在行动

本报记者　**刘　峣**

明确量刑标准

近日，国双司法大数据中心针对中国裁判文书网中2013—2016年间涉及侵犯公民个人信息类的所有刑事案件，进行了数据分析。分析显示，侵犯公民个人信息类刑事案件4年来增长近5倍。可以说，相关法律的出台恰逢其时。

6月1日，两高的司法解释生效后的首例判决，在浙江省温州市永嘉县人民法院诞生。该案被告人樊某从2015年11月开始，利用QQ聊天软件购买、交换和收集公民个人信息，并进行售卖。据樊某交待，到案发为止，他共售卖信息20万条，涉及公民姓名、身份证号码、车牌号、地址、职业等，获利约2万元。经公开审理，樊某以侵犯公民个人信息罪被判处有期徒刑3年4个月，并处罚金5万元。

姓名、身份证件号码、通讯联系方式、住址、账号密码、财产状况、行踪轨迹等，这些都属于受法律保护的公民个人信息。根据司法解释，公民个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

永嘉县法院副院长徐建宇说，《刑法修正案（九）》对侵犯公民个人信息罪的最高刑期规定为7年，但此前对于何为“情节严重”以及入罪要件尚不明晰，属于原则性规定，适用标准不统一，影响案件办理。而司法解释则对“情节严重”和“情节特别严重”作了明确规定。

司法解释就“情节严重”，明确了“违法所得5000元以上”等10项认定标准。同时根据不同类型公民个人信息的重要程度，设置了不同的数量标准。如对于行踪轨迹信息、通信内容、征信信息、财产信息，非法获取、出售或者提供50条以上即算“情节严重”；对于住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息，标准则是500条以上；对于其他公民个人信息，标准为5000条以上。

“情节特别严重”的数量和数额标准，是“情节严重”的10倍，即500条、5000条、5万条。此外，造成被害人死亡、重伤、精神失常或者被绑架等严重后果以及造成重大经济损失或者恶劣社会影响等，都属于“情节特别严重”的范畴。

“定罪量刑标准的确立有利于法律的统一、准确实施，为严厉打击侵犯公民个人信息犯罪提供了有力的法律武器。”最高人民检察院法律政策研究室副主任缐杰说。

司法解释的另一大亮点，是明确了侵犯公民个人信息犯罪的罚金适用规则。对于侵犯公民个人信息犯罪，应当综合考虑犯罪的危害程度、犯罪的违法所得数额以及被告人的前科情况、认罪悔罪态度等，依法判处罚金。罚金数额一般在违法所得的1倍以上5倍以下。

对打击侵犯公民个人信息的犯罪行为，司法解释会产生什么影响？北京师范大学刑事法律科学研究院暨法学院副教授吴沈括认为，司法解释对侵犯公民个人信息的犯罪行为提供了明确的司法适用标准。从长远来看，将有效遏制和减少生活中侵犯公民个人信息犯罪行为的发生。

他山之石

（本报记者　**刘　峣**整理）

美国　政府引导行业自律

美国采取政府引导下的行业自律，规范行业内个人信息处理行为，同时通过分散立法，辅助行业自律的实施。为了鼓励、促进信息产业的发展，美国对网络服务商采取比较宽松的政策，通过商业机构的自我规范、自我约束和行业协会的监督，实现个人信息的安全。在隐私保护和促进信息产业发展之间寻求平衡，以保证网络秩序的安全、稳定。

美国于1974年通过《隐私权法》，对政府机构收集、使用、公开个人信息和个人信息保密制定了详细的规范。而在一些比较敏感的领域，如儿童信息、医疗档案、金融数据等，美国采取分散立法形式保护个人信息。

1995年，美国提出了个人信息保护原则，随后发布《全球电子商务政策框架》，强调私营企业在保护网络隐私权中的主导作用。这一自律模式虽然在保护网络隐私权中发挥了一定作用，但是也存在一些明显的缺陷。

欧盟　国家主导统一立法

欧盟保护模式是由国家主导的立法模式，通过立法确定保证个人信息安全的各项基本原则和具体的法律规定等。

1995年，欧盟通过《个人数据保护指令》，在全欧洲范围内实行个人信息保护立法，涉及范围广，执行机制清晰。法律对进入欧盟的外企，在信息保护方面提出了很严格的要求。

此外欧盟还制定了一系列严格、完善、规范的个人信息保护法律框架，提供清晰的、可遵循的保护个人数据安全的基本原则，规范个人数据收集、处理、利用的行为。

欧盟采用两个层次的立法模式：欧盟统一立法和欧盟成员国国内立法。通过指令、原则、准则、指南等立法规制，欧盟要求各成员国建立统一的个人隐私保护法律、法规体系，保证个人数据在成员国之间自由流通，同时保证个人数据安全。

日本　综合保障安全

在借鉴欧洲和美国的信息保护模式下，日本在2005年通过《个人信息保护法》，通过这部法律全方位地实现个人信息保护。同时日本也注重行业自律和社团参与，从而形成独特的日本个人信息保护模式。

与美国类似，日本个人信息保护的发生、发展也是从地方公共团体和非政府的民间团体开始的。而个人信息保护模式上，参考了欧盟的立法模式、采纳了美国的保护规制，通过政府立法和行业自律实现个人信息安全。

1988年，日本政府制定了《有关行政机关电子计算机自动化处理个人信息保护法》，规范国家行政机关利用计算机处理个人信息的行为。

@

上海市疾病预防控制中心某工作人员利用工作便利，窃取全市新生婴儿信息并出售，累计非法获取新生婴儿信息共计30万余条；有不法分子通过互联网非法购买公民个人信息1万余条……近年来，随着互联网技术的普及，政府和企业对公民信息的收集与利用越来越广泛，由此带来的泄露风险也与日俱增。由信息泄露造成的案件多发，已成公众“痛点”。

6月1日起，最高法、最高检关于打击办理侵犯公民个人信息刑事案件的司法解释（下称司法解释）正式实施，首次针对侵犯个人信息犯罪的定罪量刑明确标准。同日施行的《网络安全法》，也对加强个人信息保护和惩治非法买卖个人信息作出了规定。

进入大数据时代，保护公民信息安全势在必行。中国正从法律入手，编织公民信息保护网。

堵住渠道漏洞

在网上购物、订机票，或是在线下租房、住酒店之后，频繁接到推销电话、短信的狂轰滥炸——这样的体验，很多人感同身受。随着移动互联网的发展，收集信息的渠道从线下走到线上，信息收集的场景与方式也越来越多，让个人信息安全面临更大风险。

中国信息安全测评中心专家委员会副主任黄殿中认为，在大数据时代，无论是购物消费、网络聊天等琐碎小事，还是买房、结婚、生子等人生大事，都不可避免地留下“数据脚印”。一旦将它们汇集整合，就会使敏感的信息迅速还原，个人隐私无所遁形。

海量数据的收集和使用，在带来诸多便利的同时，同样集聚着风险。一些互联网运营者收集了大量的公民个人信息，由于技术落后、疏于管理，对信息的监管处于松散甚至失控状态，给不法分子提供了“后门”。个别互联网公司内部员工甚至监守自盗，将个人信息非法贩卖给第三方，引发诈骗、“钓鱼”等违法犯罪现象。

360公司发布的数据显示，今年一季度，中国手机骚扰电话标记数量同比上升65.8%。骚扰电话及钱财诈骗成为威胁手机用户安全的两大方面。中国互联网协会的报告显示，2016年中国大陆网民因个人信息泄露等遭受的总体经济损失约915亿元。

专家指出，近年来，网络犯罪正向利益化、产业化、集团化的犯罪转变，出现成体系、专业化的趋势，国内国外遥相呼应，给国家和个人安全带来很大威胁。

针对信息泄露的各种渠道，司法解释与网络安全法均有针对性地提出了要求，力图堵住漏洞。

对于网络运营者因技术水平不足、管理不善导致的信息“被动泄露”，法律抬高了网络运营者门槛。网络安全法规定，网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，经过安全认证或检测后方可销售或提供。司法解释则明确，网络服务提供者拒不履行信息网络安全管理义务，致使公民个人信息泄露，造成严重后果的，应当以拒不履行信息网络安全管理义务罪定罪处罚。

而针对“内鬼”出售内部数据、获得经济利益的“主动泄露”，网络安全法规定，明知他人从事危害网络安全活动的，不得为其提供技术支持、广告推广、支付结算等帮助。司法解释也明确，在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人，数量或者数额达到司法解释规定的相关标准一半以上的，即可认定为刑法规定的“情节严重”，构成犯罪。

尹志烨作（人民图片）

构建立体防控

近年来，大数据在各行各业的应用日渐深入，显示出巨大的价值及潜力。尤其是在公共服务领域，大数据在出行、环保、健康等方面为人们的生活提供了不少便利，也为政府的管理和服务提供了依据。

与此同时，数据的风险也随之而来。专家提出，政府部门必须加大对大数据收集、存储、处理和利用过程的规制和约束。如何密织个人数据的保护网，是大数据治理进程中无法回避的挑战和课题。相关人士呼吁，要构建保护公民个人信息的立体化防控体系。

上月末，来自工信部的消息显示，中国将建立网络数据安全管理体系，强化用户个人信息保护，建立完善数据与个人信息泄露公告和报告机制。从创新防范拦截技术、突破网络安全核心关键技术等方面加强信息安全保护。

工信部副部长陈肇雄介绍，中国将重点从建立网络数据安全管理体系、强化用户个人信息保护、建立完善数据与个人信息泄露公告和报告机制3方面大力强化网络数据和用户信息保护。

专家建议，应加强对信息网络和关键领域重要信息系统的数据安全保护，明确大数据使用中各方行为体的权责义务，加强对数据滥用、侵犯个人隐私的治理和惩戒。与此同时，落实个人信息保护还需完善举报机制和补救措施，建立更加便捷的网上举报和受理制度，让泄露信息者无处藏身。

今年全国两会期间，民法总则正式通过，其中也明确了个人信息保护原则，首次从民事基本法层面提出个人信息权，并明确了个人信息保护的基本行为规范。有学者建议，下一步应推动形成系统的公民个人信息保护法律框架体系，制定专门的个人信息保护法，统一相关的法律标准和规定，明确公民个人信息保护的主体职责。

法律已齐备　落实要给力

彭训文

近年来，互联网发展越来越快，给人们生活带来了便利，也给个人信息安全带来了风险，侵犯公民个人信息犯罪行为剧增。

从今年6月1日起，公民个人信息将受到法律的空前保护。这一天开始施行的《中华人民共和国网络安全法》规定，网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息等。同时施行的《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》规定，非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息等个人敏感信息50条以上的，即构成犯罪。此外，通过“人肉搜索”公布他人个人信息，情节严重的，也要被判刑。

新华社发

长期以来，贩卖个人信息的行为让人深恶痛绝。从刑法修正案（七）到刑法修正案（九），中国都在逐步完善维护公民个人信息安全的法律规定。但是在司法实践中，如何界定公民个人信息范围、如何认定非法提供公民个人信息的标准、哪些情形即可构成侵犯公民个人信息犯罪、哪种情形属于侵犯公民个人信息犯罪情节特别严重等，却不太明确。标准不清晰，不仅在客观上影响了打击成效，也给一些不法人员提供了打法律“擦边球”的机会。

此次实施的网络安全法和两高司法解释，对上述司法实践中出现的问题和“模糊边界”进行了明确界定。比如，两高司法解释明确，非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息500条以上，即构成犯罪。这意味着，那些长期打着合法经营旗号，非法出售、获取公民个人信息的行为已经构成犯罪，公众今后完全可以向公安机关进行举报。

不过，要形成打击合力，既要靠法律规定的完善，也需要相关部门的贯彻落实。司法部门需要改变观念，重拳出击，加强执法力度。那种以“实际损害”为判断依据的老习惯显然已不合时宜。须知：侵犯公民个人信息，不在损失金额多少，而在于公民个人信息被“暴露”后所受的精神伤害。只有认识到这一点，司法人员在今后面对这些案件时才能显得更加积极有力。

同时，公民的个人信息不会直接飞到贩卖者手中，一些社会机构是实质上的间接责任者。因此，这些搜集公民个人信息的社会机构自身需要做好管控，严防严查那些顶风作案、知法犯法的“内鬼”出现。此外，用第三方力量对这些机构进行严格监管也很有必要。

总之，如今法律条件已齐备，下一步的落实要得力，态度要坚决。实践告诉我们，社会法治大环境的改变是一个有机的连锁递进过程，这需要其中各方发挥好自身作用，同时督促好其它各方也要切实发挥作用。只有这样，新法才能产生真正的威慑力。