

隐私保护需开放合作、透明监督

斩断黑色产业链 上海检方探索建立“侵犯公民个人信息案件检察官办公室”

□法治报记者 夏天

近期华住集团旗下酒店数据被窃案，引起舆论一片喧哗，从中也折射出我国个人信息保护的短板。

在当前的大数据、人工智能背景下，上海检察机关已经注意到，目前专门从事个人信息搜集与买卖的产业链层出不穷——产业链顶端是行业“内鬼”或网络“黑客”，通过登入或侵入政府、企业的内部系统非法窃取各类个人信息。随后，网上“信息二道贩子”将公民个人信息当作商品在网上兜售。

目前，上海检察机关正探索建立更具专业性的“侵犯公民个人信息案件检察官办公室”，力争为群众提供更优质的检察产品。而在全市层面，市委网信办已高质量的在全市范围内开展关键信息基础设施网络安全大检查，并以网络安全检查为基础，构建网络安全工作机制，打造动态感知网络安全态势的技术平台，建立关键信息基础设施信息库，完善全市网络安全保障体系。



针对网络信息安全保护，越来越多的人已意识到齐抓共管形成合力的重要性
本版摄影 记者 王湧

业界之困

银行衍生百亿“黑产” 如何构建安全生态

在上周举行的“2018 年国家网络安全宣传周上海地区网络安全高峰论坛”，浦发银行科技部总经理蒋瞳介绍了银行业面临的信息安全挑战：“近两年来网络攻击呈现出明显的几大特征：第一个是人员组织化，第二个是资源全球化，第三个是动机利益化，还有活动的常态化。”

蒋瞳举例，比如实施 ATM 吐钞事件攻击的“黑产”集团，就是依托互联网分工协作的方法进行攻击。在这个过程中，也形成了各种各样的黑客组织。据统计，仅国内的非产业从业人员就已超过四十万，每年从中的获利有上百亿。

然而，现在的银行业防护体系，在新的挑战下强度不够。安全防护体系仍然偏单点防御、被动防御、静态防御，对于综合性、连续性、精准性的攻击没有形成充分动态的纵深防御体系，无法充分应对上述攻击形式。

从保护对象来看，银行需要保护的信息资产日益复杂，随着银行规模的扩展，个例如浦发银行，资产规模达到 6 万多亿，各类信息资产日益增多，加大了信息安全的防护难度。

银行业线上化趋势也越来越快，使得柜面工作被机器替代了 90%。如浦发银行，这两年运营成员从 6000 多人减到了 2000 多人，

取而代之的是越来越多系统跟互联网的紧密相连，此外跨界合作的第三方机构的互联互通更加普遍。但上述信息化成果，均扩大了系统被攻击、破坏的面积。

蒋瞳认为，大数据、云计算、物联网、人工智能、区块链等等，这些技术模式的应用，都会带来在系统、网络、数据层面的威胁。“因此当前网络安全防控最重要的，是安全边界的划分和安全边界的识别，以及在这种边界情况下的保护。我们要构建安全生态，需要大量合作伙伴，我们外包合作者、合作伙伴越来越多，传统边界防护的思路已经不能适应新时期的要求了，边界防护越来越经受挑战。”

上海倡议

隐私保护需开放合作、透明监督

在业界和司法界，针对网络信息安全保护，越来越多的人已意识到齐抓共管形成合力的重要性。而在上周举行“2018 世界人工智能大会·人工智能安全高端对话”上，一封联合了国内外人工智能安全领域的专家学者和产业界人士的“上海倡议”，就体现出一种“安全生态”的雏形。

在《人工智能安全发展的上海倡议》中，提出了“隐私保护”，呼吁人工智能发展需要保障用户的数据安全，人工智能发展不得以牺牲用户隐私为代价，需要加强数据保护立法，丰富人工智能的技术路线，不断强化人工智能应用中的用户隐私保护。

倡议提出“透明监管”，呼吁

人工智能发展应当避免技术黑箱导致的安全风险，需要通过建立可审查、可回溯、可推演的监管机制，确保目标功能和技术实现的统一。

倡议的最后提出“开放合作”，呼吁人工智能发展需要各国、各方的协同共进，应当积极在国际范围建立人工智能安全发展的规范和标准，避免技术和政策不兼容导致的安全风险。

无独有偶，网络安全周上，阿里巴巴等 12 家大数据企业，在杭州签署了《个人信息保护倡议书》。倡议书提出，公开透明处理用户信息。用通俗易懂的语言、简单直观的方式，向用户明示个人信息处理目的、方式、范围、规则等；同时，不使用“一揽子协议”的方式

强迫用户打包授权对个人信息的收集，为用户提供个人信息申诉渠道、注销账户或关闭的途径；建立可访问、更正、删除其个人信息处理机制。不超范围和约定，收集、存储、使用、共享个人信息；在个人信息处理活动时，对用户合法权益造成的损害依法承担责任；一旦发生重大个人信息泄露事件及时告知用户。

建立用户信息安全屏障成为倡议书的重要内容之一。12 家大数据企业承诺，遵照国家相关标准要求，采取充分有效的安全技术和管理措施，防止个人信息泄露、毁损、丢失。加大个人信息保护技术的创新，加强网络安全产品的研发和应用。

检方发力

探索建立“侵犯公民个人信息案件检察官办公室”

8 月 28 日被公之于众的“黑客出售华住酒店集团客户数据”一案，其中涉及姓名、身份证号、手机号、邮箱、家庭住址、开房记录、登录账号密码等敏感信息，多达 5 亿条信息，打包价为 8 比特币，约合人民币 38 万元。这批数据涉及华住集团旗下的汉庭、桔子、全季、星程、海友等 10 余个品牌酒店的住客信息，数据截止到 2018 年 8 月 14 日。

有业内律师表示，此次涉及的个人信息不仅数量巨大，而且涉及大量敏感信息，若查证属实，将是迄今为止最大最严重的酒店信息泄露事件。

日前，利用黑客手段窃取华住集团旗下酒店数据，并在境外网站兜售（未交易成功）的犯罪嫌疑人刘某某，已被上海警方抓获归案。长宁区人民检察院第一时间指派互联网犯罪检察官办公室提前介入该案，引导公安机关侦查取证，切实保护公民合法权益。

其实近年来，侵犯公民个人信息的违法犯罪屡见不鲜，波及的公民年龄层甚至已下探到新生儿——据市检察院披露，在 2014 年初至 2016 年 7 月期间，上海市疾病预防控制中心每月更新约 1 万余条新生儿信息，却被中心工作人员韩某利用职务便利，在这一时间段内窃取了共计 30 万条全市新生儿信息并转卖给张某某、范某某等人。浦东新区人民检察院于 2016 年 11 月 22 日，以侵犯公民个人信息罪，对韩某等人提起公诉。2017 年 2 月 8 日，浦东新区人民法院以侵犯公民个人信息罪，分别判处韩某等

人有有期徒刑 7 个月至 2 年 3 个月不等，并处罚金 2000 元至 5000 元不等。

市检察院表示，由于信息被视为“数字时代的石油”，公民个人信息经济价值日益显现，导致上下游犯罪密切勾连形成黑色产业链。产业链顶端是行业“内鬼”或网络“黑客”，通过登入或侵入政府、企业的内部系统非法窃取各类个人信息。接着，网上“信息二道贩子”创建诸如“车主信息”“患者信息”“网购物流信息”“股民信息”等 QQ 交流群，将公民个人信息当作商品在网上兜售，这是目前公民个人信息倒卖的主要渠道。

市检察院表示，针对侵犯公民个人信息案件，上海检察机关注重建立专业化办案机制。因为侵犯公民个人信息案件具有信息化高、技术性强的特点，上海正结合司法体制改革和办案责任制落实，探索设立办理侵犯公民个人信息案件的检察官办公室，加强对检察官的信息科技知识、办案应诉技巧等方面的培训，使其能够适应新时代办案需要，为人民群众提供更优质的法治产品、检察产品，通过办案满足人民群众对安全感的需要。

市检察院还建议，可完善多部门联动、衔接的工作机制。公民个人信息保护涉及工业信息部门、公安部门、银监部门、工商部门、税务部门、电子商务运营商等各种主体，各部门需要明确责任分工、齐抓共管共建，健全工作衔接协作机制，通过建立信息共享平台、定期召开联席会议等多种途径，加强工作联动，促进形成公众自觉、行业自律、政府监管、司法监督的公民个人信息保护体系。