保护个人信息将出台行业标准

由工信部牵头30多家单位起草，正报批国家标准；为企业处理个人信息提供行为准则

个人信息安全之动态

近日，工信部直属的中国软件测评中心透露，他们联合30多家单位起草的《信息安全技术、公共及商用服务信息系统个人信息保护指南》已正式通过评审，正报批国家标准。

工信部安全协调司副司长欧阳武介绍说，这个指南能为行业开展自律工作提供了很好的参考，为企业处理个人信息制定了行为准则。据介绍，我国信息技术保护不容乐观，甚至已形成利用个人信息从事非法获利的黑色链条。特别是去年年底揭露出的中国互联网最大规模的泄密事件，将个人信息保护推向了风口浪尖。

许多发达国家很早已开始个人信息的保护研究和立法工作。我国近年来也启动了个人信息保护的相关工作。

去年，全国信息安全标准化技术委员会提出制定个人信息保护指南。这个委员会主要从事信息安全标准化工作，现任主任由工信部副部长杨学山兼任。

个人信息保护指南的全称是《信息安全技术、公共及商用服务信息系统个人信息保护指南》，标准由工信部直属的中国软件测评中心牵头，联合近30家单位起草。

该中心常务副主任黄子河透露说，指南目前还在等待批准文号，但其最终的发布应是“指日可待”。但这个指南并非国家强制性标准。

■ 焦点

个人信息用后立即删除

在个人信息安全缺少专门法律规范时，一部行业标准成为业内的希望。

“去年正式通过了评审，报批国家标准”，中国电子信息产业发展研究院院长、中国软件评测中心主任罗文希望今年能通过这项标准，以拓展个人信息保护的体系。

《个人信息保护指南》对个人信息的处理包括收集、加工、转移和删除四个主要环节，其中还提出了个人信息保护的原则。

工信部安全协调司副司长欧阳武介绍，“这个原则包括目的明确、最少使用、公开告知、个人同意、质量保证、安全保障、诚信履行和责任明确等八项。”

“最少使用”的原则就是获取一个人的信息量时，只要能满足使用的目的就行。

黄子河举例说，一些网站本是办一个很小的事，却让用户填包括家庭住址、手机号在内等很多信息，这就不符合“最少使用”原则。

“安全保障”则是要个人信息管理者一旦收集了个人信息，就必须建立一套个人信息保护制度，明确责任人和内部管理流程，以及应对个人信息泄露的风险。

中国软件测评中心的副主任高炽扬估计，个人信息泄露中70%-80%属内部作案，这是“安全保障”原则没能落实好所致。

他介绍说，一些商业公司掌握大量个人信息，由于管理制度疏漏，一些内部员工未经授权就能获取客户信息。

依照《个人信息保护指南》，在收集个人信息阶段告知的“使用目的”达到后应立即删除个人信息。

高炽扬说，有次，他在某航空公司网站购买机票，使用电话支付的时候，工作人员搜集了他的支付信息：姓名、身份证号、信用卡号和信用卡的最后三位支付号码。购票成功。

但是，过段时间他再去购票时，对方问他，“您还是使用卡号末四位是****的信用卡支付吗？如果是，只要告诉我就可以了。”

“(这家公司)存储了我的信息。”3月26日，高炽扬一边讲述一边摇头。

高炽扬说，他所经历的航空公司电话订票的经历，就是航空公司在达到此次订票目的后，未能及时删除客户信息。

信息保护指南非强制标准

“为了经济效益，无利不起早。”高炽扬估计，目前没有哪个行业不存在信息泄露。

比如孕妇生完孩子刚回家，卖奶粉的电话就过来了，病人检查完身体，检查单还没看懂，相应的医药公司就已经打电话卖药来了。

中国软件评测中心研究员刘陶把个人信息比喻成“很多钱装在纸糊的银行里，很容易被黑客破解。”据他们调查，公众最关心的金融、电信等领域的个人信息安全。

而让人担忧的是，这个指南标准不是强制性标准，甚至也不是推荐性标准，标准通过会对行业起到多大的规范效力，仍待观察。

中国软件评测中心主任助理朱璇说，此次个人信息安全国家标准“属于技术指导文件”。

国家标准分为三种，一个是强制性标准，一个是推荐性标准，一个是指导性技术文件，标准可以作为参考。而国家强制性标准多在食品安全领域。

不过，黄子河认为，标准适用于除了政府机关等行使公共管理职能以外的各类组织和机构，特别是电信、医疗等涉及个人敏感信息比较多的服务机构。

昨日，一位乘客用手机扫描自己的火车票信息。通过扫描软件可获得火车票二维码含有的身份证信息。 本报记者 浦峰 摄

■ 现状

40部法律难约束个人信息泄露

工信部电子科技情报研究所副所长刘九如统计，目前有近40部法律、30余部法规，以及近200部规章涉及个人信息保护，其中包括规范互联网信息规定，医疗信息规定，个人信用管理办法等。

“针对个人信息的法律法规并不少，然而内容较为分散、法律法规层级偏低。”刘九如说。

刑法修正案(七)被认为是个人信息立法的标志性事件之一。

2009年，刑法修正案(七)确定了“出售、非法提供公民个人信息罪”、“非法获取公民个人信息罪”罪名，首次将公民个人信息纳入刑法保护范畴，规定要追究泄露、窃取和售卖公民个人信息行为的刑事责任。

但是，这一犯罪主体是“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员”。除此之外，还存在着互联网公司、房地产公司、物业公司、汽车厂商、宾馆酒店、会计师事务所等掌握个人信息的机构和单位。

诸多法律界人士认为，刑法未明确该罪的具体界定标准，这一条款还有进一步改进和完善的空间。

另外，专家认为法律中对信息泄露者惩罚机制不够。

前段时间，警方破获CSDN(即中国软件开发联盟)的600多万条用户名和密码泄露案件，“目前为止对网站的处罚只是提出行政警告，太轻了，这种处罚几乎没有威慑力。”北京科技大学经管学院教授梅绍祖说。

梅绍祖认为，如果在国外，这样的大规模用户信息泄露，至少应该有经济处罚。

2009年，《侵权责任法》的通过，使“人肉搜索”侵犯受害人权利的责任认定有了法律的统一规制，如果网站无视受害人提出的屏蔽、删除要求，就要承担连带责任。

但是，社科院法学所研究员周汉华说，《刑法》和《侵权责任法》都属于事后救济，在网络时代要对网络安全以及个人信息进行全流程的监管才更为有效。

个人信息安全法未入立法程序

《个人信息安全法》并非从未尝试破冰。

工业和信息化部副部长杨学山回忆，2003年的4月，国务院信息化办公室专门对个人信息立法研究课题进行部署，2005年《个人信息保护法》专家意见稿已经提交。不过这项立法建议一直未能进入正式的立法程序。

参与此次专家意见稿的梅绍祖说，当时文本已从国务院信息化办公室上报到国务院法制办，此次未能进入正式立法程序的原因很复杂，主要是“从紧迫性上讲还没太关注这个问题”。

梅绍祖承认，凡事总有轻重缓急，有关部门会综合考虑，但考虑到目前我国发生的个人信息泄露和被盗、个人隐私侵犯以及个人信息交易的事件愈演愈烈的现实，再发展下去可能会影响到整个社会经济活动，“我觉得紧迫性早就有了，可能各个层面感觉不一样，有人觉得没那么紧迫”。

工信部副部长杨学山力主加快立法。

他说，个人信息保护实行面广，一定要从法的角度规范，才能使这项工作在法律上有依据。

“这几年我们和大家一起在个人信息立法尽快进入正式程序正在努力。”杨学山说，在大家的努力下，“尤其是在今天个人信息保护已经成为社会迫切的问题，立法的进程就会加快”。

A06-A08版统筹：涂重航
本版采写/本报记者 郭少峰 吴鹏

责编 涂重航 图编 杨杰 美编 李铁雄 责校 田秋霞