■整治电话诈骗

徐玉玉案应成为大数据时代的“坐标”

社论

临沂女孩徐玉玉遭遇电信诈骗，郁郁而终，经过警方的全力侦查，此案已于昨日告破。这个消息让人悲喜交集，喜的是正义伸张在即，悲的是早逝的生命并不会因此挽回。唯有以此案为起点，唤起全社会对公民信息安全的重视，推动相关立法的启动，才能告慰死者，并避免后来者重蹈覆辙。

媒体最初爆出徐玉玉案时，有人还感叹死者太单纯。但是从相关信息中可以看出，犯罪嫌疑人实施了非常精准的诈骗手段，即使有相当社会经验的人也未必能确保不受蛊惑，何况受害人还是涉世未深的学生。有媒体在报道中披露，有技术人员猜测，犯罪嫌疑人能如此准确地掌握受害人的个人信息，很可能先有黑客入侵相关系统，然后把所窃取的信息贩卖给了别有所图的人。这种黑色利益链让人不寒而栗。

现在，几乎每个人有无数的个人信息被各种机构记录保存。可以说，一个人从出生就开始了数字化生存，他的饮食、医疗、出行、购物等行为产生的数据被很多机构以各取所需的方式采集，以此为基础，大数据又推动了“私人定制”。在大数据时代，数据就是财富，甚至有人认为，未来所有的生意都是数据生意。正是因为认识到大数据和互联网已成为产业发展的创新要素，国家大数据战略在去年开始实施，以推进数据资源共享。

大数据带来的大产业、大机遇、大红利，很多人深有体会，与此同时，我们也越来越清晰地感受到大数据带来的大风险。我们很多人几乎每天都会接到很多莫名的电话，对方不仅知道你姓甚名谁，还了解你的资产状况和个人爱好。我们像“透明人”行走在信息社会，却不知道致命的“暗箭”会从哪里袭来。究竟是谁出卖了我们？个人凭一己之力已经很难追溯源头，因为各个环节都有失守的迹象。以徐玉玉案为例，教育部门的助学金信息何以泄露，虚拟运营商怎么使得“实名制”有名无实，诈骗分子在银行的账号又是如何开设的，这些问题都让公众感到困惑。如果所有联网的信息都可以被人恶意共享，那么个人财产受到侵害并非最严重的后果，更严重的可能会危及国家安全和社会稳定。鉴于恐怖袭击已经呈现全球化趋势，这种担忧绝非杞人忧天。

徐玉玉案从案发到告破，只是一周时间。很多人眼中的这桩“悬案”，因为得到足够的重视，没有再无解。由此也给人启示，只要思想上重视，行动上积极，在大数据时代完全能够有力地打击那些窃取数据为非作歹的行为。与事后清理相比，源头预警其实更为重要。目前世界上已有多个国家立法保护个人信息，而我国还没有一部完整的个人信息保护法。虽然刑法中有惩处“违反国家有关规定，向他人出售或者提供公民个人信息”的条文，但是对个人信息的保护，现在亟待推进专项立法，进行更明确更严格的约束和惩罚。这也是对公民个人信息保护应有的顶层设计。

在徐玉玉离世之后，媒体又报道，临沂还有一名大学生也因遭遇电信诈骗伤心过度而去世。在电信诈骗已近泛滥的今天，我们不知道下一出悲剧会不会上演。历史的最大无奈就是“后人哀之而不鉴之，亦使后人而复哀后人也”。每一个个体生命的逝去都让人哀伤，如果他们的牺牲还能推动社会不断取得进步，这才是悲喜交集，否则就是空悲切。所以，我们期待徐玉玉案能成为大数据时代的一个“坐标”，推动各界加快立法进程，不让它成为被人淡忘的一段谈资。

大数据发展还缺信息安全护航

个人信息裸奔，一年损失900多亿

临沂女孩徐玉玉遭遇电信诈骗，再次引发全民对个人信息泄露的恐慌。大数据时代，个人信息保护立法不完善，个人数据基本处于“裸奔”状态。当下大数据产业成为香饽饽，国家层面鼓励数据开放，同时数据安全和个人隐私保护也亟待规范。

本报记者　韩笑　整理

手机实名制难落实 银行发卡也泛滥

中国互联网协会《中国网民权益保护调查报告2016》显示，近一年的时间，国内6.88亿网民因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算达915亿元。

网络非法获取公民个人信息日益猖獗，涉及身份信息、电话号码、家庭地址，扩展到网络账号和密码、银行账号和密码、购物记录、出行记录，且形成了“源头—中间商—非法使用人员”的黑色产业。机关单位、服务机构以及个体企业相关人员参与的泄露活动更加隐蔽，而通过技术手段实施攻击、撞库或利用钓鱼网站、木马、免费WIFI、恶意APP等技术手段窃取成为重要的泄露方式。

今年4月以来，公安部部署开展了打击整治网络侵犯公民个人信息犯罪专项行动，截至7月全国公安机关已累计查破刑事案件750余起，抓获犯罪嫌疑人1900余名，缴获信息230余亿条，清理违法有害信息35.2万余条，关停网站、栏目610余个。

不少网络诈骗犯罪团伙拥有大量电话卡和银行卡，说明运营商实名制没有完全落实，很可能存在一些员工非法寻租、参与犯罪。银行也存在发卡泛滥，实名制未落实、银行网络在境外转账分解资金缺乏限制等现象，这些是导致电信诈骗案猖狂肆虐的根源所在。

业内人士认为，手机号码层层渠道分销，由于一些营业厅业务繁忙，每天办卡业务近百起，工作人员在检验办卡人能否和身份证对上时，难免有疏漏、失误，或者一些乡镇的地方营业员工作态度不过关，很难确保100%实名，何况还有犯罪分子能用非法软件破坏实名登记。实名制只是一定程度上提高电信诈骗成本，但不能治本。

教育局网站 敲几个回车就侵入

由于普遍不具备经济能力，学生群体并非电信诈骗的重灾区，但学生信息却堪称“最没有安全保障”的一类。

近日，记者接触到数个倒卖用户数据的业内人士。其中1人向记者展示的上海某知名大学数据，包含了学生姓名、学号、性别、年龄、身高、体重、联系方式、专业等详尽信息。

此外，该人士表示可以拿到“全国中小学生学籍信息管理系统”，包括学籍号、学校、入学方式、住址、家庭成员等等。该人士称，“国内学校，有一半数据我都有。即使手头没有的，只要你告诉我名字，我也都能拿到。”

根据多位人士报价，“新鲜出炉”、“没有卖过”的一手学生数据，售价约1-2元/条，大量采购还有优惠。而二手的数据，基本低于1毛，如果批量购买，1万条二手数据约300-500元。在整个数据黑色产业领域，学生数据售价偏低，相比之下，一些从淘宝、京东、唯品会等电商平台流出的一手数据，售价在3-5元。

“倒卖生源数据的漏洞长期存在。很多民办大学会借合法专业的名义搞非法成教、网教来招生。”一位北京某学校教师告诉记者，对于开设成教、网教教育的学校而言，“高分学生数据不值钱，都是白送，分数低的才值钱。拿到数据之后，学校安排话务组开始打电话，几天就能招50-60人。有的学校每年因此盈利上亿元。”

学生信息泄露，有些是因为接触数据的工作人员所为，有些则是黑客入侵获取。

当下新兴的大数据交易被人担忧缺乏数据隐私方面的监管。（资料片）

多位信息安全领域的权威人士表示，教育行业的信息安全能力普遍极低。随便一个入门的黑客，都能搞定绝大多数学校、教育主管部门的系统，几乎不耗时间，甚至只需要敲几下回车就可以。

有些数据交易 打了法律擦边球

进入移动互联网时代，大数据的价值被放大，而人们日常生活场景却都与数据有关。

白领小王早上起来跑步打开咕咚，买早餐用微信支付，上班打开滴滴，上网打开微博，发微信朋友圈，午餐用百度外卖，淘宝下单买袜子。一天下来，个人的健康、家庭住址、活动路线、电话、办公地址，以及性别、体重、饮食习惯，甚至身份证号码都曝光到了相关平台。

基于这些数据，相关平台可以将我们的个人信息数据化。商家可以根据小王们的信息，精准投递广告，做互联金融征信，甚至卖数据。

据报道，2015年底，浙江省高级人民法院与阿里巴巴集团达成战略合作，通过淘宝平台的数据锁定当事人常用电话和地址，把法律文书寄往淘宝收货地址，提高送达率。另外，浙江高院可利用阿里平台的海量数据，对在该平台上留下数据的涉诉人员绘制“画像”，包括身份信息、联系信息、消费数据等。

“通过黑市可以买的数据不是什么秘密的信息。”中关村一家大数据企业高管介绍，数据黑市主要是指法律明确禁止的一些数据的交易，目前有一些法律明确的客户隐私信息数据，是不允许公布的，还有一些法律并没有明确的，但是在道德层面上不允许公开的数据。

上述高管透露，个人乘坐飞机的记录，还有通讯运营商的数据、银联的数据，大多都可以通过黑市买到。

某电信运营商中层表示，大平台对个人数据的保护相对规范，其对个人数据的使用和交易，会采取脱敏处理，但是目前一些小的平台就很难说，即便是个人数据被出卖，也很难取证和维权。

在大数据淘金热的驱动下，地方层面近两年也在探索个人隐私保护。今年年初，贵州省通过《贵州省大数据发展应用促进条例》，是中国首部大数据地方法规，但遗憾的是，这部法规重在鼓励地方建产业园区，关于数据隐私安全，以及数据交易方面，并无具体涉及。而业内估计，2016年，我国大数据交易市场规模将超过60亿元，到2020年有望超过500亿元。

上海政法学院经济法学院副教授肖卫兵表示，目前国内相关研究并不成熟，未来发展方向不清晰，立法不可能走在实践前面；同时国家层面立法不清晰，地方在敏感领域的突破比较难。清华大学数据科学研究院执行副院长韩亦舜表示，在个人数据隐私保护方面，建议地方多尝试探路，立法都是在实践后面。