侵犯公民隐私信息案频发，实名制的“副作用”谁管？专家认为——

个人信息不能网上裸奔

本报记者　彭训文

针对引发公众关注的“记者花700元买到同事行踪”报道，12月17日上午，公安部发布消息称，已查明此案是由相关单位内部人员与社会人员相互勾结所为，3名涉案人员已被抓捕归案。

如今，互联网信息进入大爆发时代，公民个人信息从线下转移到网上。同时，被称为“最严厉的登记政策”——“实名制”在中国通讯、保险、银行等各行业深入推进。

如何保证这些登记在册的隐私信息不成为犯罪分子实施精准诈骗的工具？多名网络法专家、社会学家在接受本报记者专访时表示，在没有对公民个人信息进行严密保护的情况下，要充分考虑实名制信息泄露后可能带来的负面危害，对相关机构、责任人采取更多有针对性的制约手段。

十一月月二十九日，广东省公安厅组织千警摧毁多个电信诈骗犯罪团伙。图为查获赃物现场。　本报记者　贺林平摄

贩卖个人信息向纵深发展

你所有的隐私信息，包括开房记录、名下资产、乘坐航班，甚至网吧上网记录信息，只要有人付钱，就可以轻易被查到。换句话说，你的个人信息正在网上“裸奔”。据《南方都市报》此前报道，该报记者在网上花了700元就查到了同事的上述隐私信息，同时还能查到国内四大银行存款记录、手机实时定位和手机通话记录。更可怕的是，整个交易已跃升到了“平台化”地步。

全国公安机关今年合力开展打击网络侵犯个人信息犯罪专项行动后，抓捕了多名行业内鬼、黑客。但是，问题并未得到根本解决。

“如今的网络侵犯公民个人信息犯罪已经向纵深发展了。”中国传媒大学文法学部副部长、网络法与知识产权研究中心主任王四新在接受本报记者采访时表示，这个案件已经不是简单的出卖个人隐私信息的问题了，还可能牵涉到一些机构、人员。“不能排除相关正规酒店、个别地方公安机关参与其中，因为很多数据只有这些机构才可能获得。”

这起案件中，犯罪分子以标准化形式向市场提供公民个人信息。王四新认为，这说明犯罪分子在打通其中关节方面已经做了很多工作，形成了倒卖个人隐私信息的黑色产业链。“如果商业力量和行政力量形成耦合关系，这是非常可怕的。”

“现在的问题是有利益，有市场，但是缺监管。”中国人民大学社会与人口学院教授陆益龙对本报记者表示，公民个人信息被非法利用现象之所以猖獗，一是公民个人信息非法交易市场的存在。一些犯罪分子能够通过网络空间，非法倒卖公民个人信息以获得非法利益。二是一些采集、使用公民个人信息部门的安全责任意识缺失。这些部门、机构要求公民提供详细的个人信息，但是没有履行好防止这些信息被非法利用的职责。

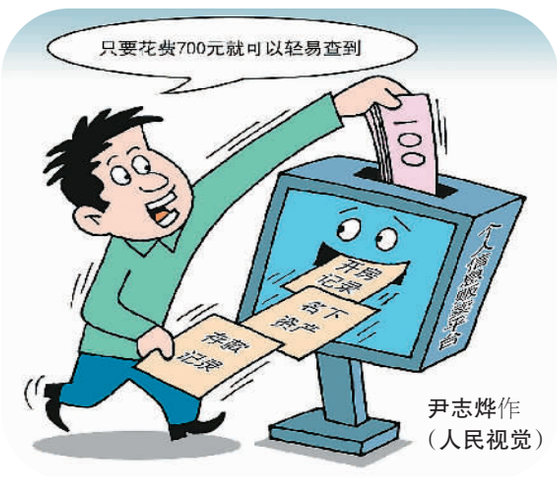
此外，陆益龙认为，目前法律对如何使用和保护个人信息缺乏强制性、有约束性的规范和措施，造成个人信息交易猖獗，“2003年，我国就开始起草《个人信息安全法》，2005年又提交了《个人信息保护法》专家意见稿，但这么多年过去了，这些法律实质进展到什么程度了呢？”

实名制信息泄露的“锅”谁背？

今年12月12日，中国社会科学院发布的《社会心态蓝皮书：中国社会心态研究报告（2016）》显示，食品安全和个人信息安全是目前公众最为担心的问题。

现代社会讲究“无互联网不社交”，很多人习惯将个人信息放入“云端”，但问题是，这个云端真的安全吗？据中国互联网协会发布的《2016中国网民权益保护调查报告》显示，84%的网民曾亲身感受到由于个人信息泄露带来的不良影响。

陆益龙分析称，安全需要是人的最基本需要，公众之所以对公民个人信息保护特别担忧，主要是近些年电信诈骗犯罪分子利用这些信息大大扩展了犯罪侵害范围，让越来越多的民众成为受害者。



尹志烨作（人民视觉）

上个月公布的《网络安全法》明确提出，将严厉打击出售贩卖个人信息的行为。让王四新担忧的是，如何防止一些人知法犯法，“现在很多行业机构的相关人员卷入网络侵犯公民个人信息的案件，这不仅极大地打击了公众对个人信息最起码的安全感，更会对社会信用体系建设造成严重影响，同时会降低海外对中国维护网络信息安全的信心。”

为防止犯罪分子利用个人信息实施电信及网络诈骗，国内已经推行了几年的“手机实名制”，要在今年年底画上句号。国家6部委此前联合发布的《防范和打击电信网络诈骗犯罪的通告》强调，到2016年底前，全部电话实名率要达到100%，在规定时间内未完成真实身份信息登记的，一律予以停机。

据此，11月底，北京已经对“非实名制”电话实施“双停”（不可接听不可打出），2017年1月底“非实名制”电话将被“销户”。目前，全国很多省市都在根据各自情况陆续推进此项工作。

同时，银行、交通、宾馆和民航等部门正推行通过连接公安个人身份认证系统来验证个人信息，还有人提出通过推行“一号通”来加强网络平台个人信息安全管控。

但是，一方面，实名制只是增加了骗子的犯罪成本，并不能直接解决问题。中国移动相关负责人表示，电信运营商推行实名制，确保的是手机用户和身份证的匹配一致性，至于这个身份证是不是本人，光靠运营商不能百分之百肯定。另一方面，一些采集、使用公民个人信息的行业在确保数据库安全方面投入不大，相关数据屡次被黑客以“撞库”方式盗取。更为严重的是，一些行业工作人员因为利益诱惑甘当内鬼，勾结不法分子倒卖个人信息数据。

国家检察官学院沈海平教授对此强调：“在没有同时对个人信息进行严密保护的情况下，要充分考虑实名制信息可能泄露带来的负面危害。”

“中国目前还有将近一半的人没用上互联网，即使所有公民在网络空间都实名化了，同样可能存在虚假信息问题。”王四新同时认为，商业机构内部当然会不遗余力地抓内鬼，但是他们对于对公民个人信息数据的保护也是有商业利益诉求的。“要打通不同网络平台间在商业性个人信息数据和政务性个人信息数据之间的界线，需要政府相关部门想清楚，哪些数据是基于公共利益的需求可以直接征用的，哪些是需要给予补偿的。”

“同时，如果商家将这些数据和政府分享，如何避免新环节里的内鬼？数据跨平台流动后，如果出现问题，谁来承担相关责任？”王四新说。

综合治理才能斩草除根

鉴于利用个人信息进行的电信、网络等新型违法犯罪不断出现，公安部网安局已决定，将今年4月底开展的为期6个月的打击整治网络侵犯公民个人信息犯罪专项行动延长至2017年12月底。中央网信办相关负责人近日也表示，将统筹协调各相关部门开展打击整治行动。

如何使下一阶段的打击行动更有针对性，起到斩草除根的效果？王四新认为，公安部门应该对整个倒卖公民个人信息的产业链进行查处，搞清楚有哪些机构和人员卷入、链条上各部分是如何分工配合的。“我们还要特别关注受害者群体，弄清楚他们是如何受害的，对他们的个人和家庭生活造成了什么影响，如何重振他们对商业结构、政府机构乃至整个社会的信心等等。”

“要遏制住网络侵犯个人信息和电信诈骗犯罪蔓延势头，需要相关部门采取一些霹雳手段。”在陆益龙看来，网络监管部门应该对相关采集、保管个人信息的平台设置准入门槛，“安全数据库技术上不达标的，一票否决”。

对于用户因个人信息被窃取而出现的资金损失，金融系统、移动或网络支付平台间常常“互踢皮球”。陆益龙认为，大量电信诈骗犯罪分子将魔爪伸向中国百姓，与银行系统乱发银行卡、相关平台对转账技术的管控不力有很大关系，应督促这些部门、平台提升安全技术，并责成其停止已经对公民信息安全产生严重负面影响的促销方式。

更多网络安全方面的专家认为，解决个人信息安全问题是一项社会化、系统化的工程，目前亟须通过立法，对公民个人信息安全保护进行强制性规范，以促进社会各方的综合治理。

“对于侵犯个人信息别总在末端治理，强化源头管控与预防更为重要也更加关键。”王四新认为，应该通过立法确立相关机构对公民个人信息的管理责任，促使各行业依照法律构建内部管理规则和安全责任体系，同时也让更多公民在使用互联网时知道如何保护自身合法权益。

“我们需要在全社会构建起网络信息安全的法治体系。希望将来即便出现侵犯个人信息的案件时，相关部门能够快速启动应急措施，断开相关链接，把公民的损失降到最低。”王四新说。

从垃圾短信退订说开去

刘　嶢

基于移动互联网的各类应用极大便利了我们的吃穿住行，但同时也带来了不少让人烦恼的副产品。垃圾广告短信就是其中之一。

曾经购买过的网店上新品了、网约车平台有了新优惠、银行办信用卡送大礼……只有你想不到，没有垃圾短信发不到。其中，不少垃圾短信的发送者是一些闻所未闻的品牌或商家，他们能准确地报出你的网名或真名。显然你的个人信息又被“卖”了。

一眼看去，这些推销性质的垃圾短信似乎并没有那么“糟糕”，大部分短信末尾都按照规定写明了用户退订的方法，例如“回复TD退订”“退订回N”等。然而，与垃圾短信交手多了就会发现，其中的浑水之深，套路之多，超乎常人想象。

比如，某网约车平台，用户回复退订短信后，平台又换个号码锲而不舍地骚扰用户；某些商家所谓的退订方法完全无效，用户根本无法通过正常渠道退订；有的短信称“回复T即可退订”，用户尝试了半天，竟发现要发送“复T即可”才能退订。跟“上帝”般的用户玩这样的文字游戏，简直令人怒不可遏。

其实，广告类垃圾短信花样翻新的背后，是用户信息泄露严重的客观写照。数据显示，在4.8亿的网购用户中，过半遭遇过个人信息泄露。

泄露的源头在哪里？一是电商、快递企业的员工，将工作中收集的个人信息出售牟利，监守自盗当“内鬼”；二是一些电商平台成了信息贩卖的中转站，用户的信息按利用价值明码标价；三是很多电商平台过度收集个人信息，对个人信息的保护不上心、不积极，有人形容“买个酱油都得提供姓名、住址、身份证号码”。

细细想来，这些垃圾短信，消费者根本未曾“订阅”，何来“退订”之说？开开心心网络消费，却不明不白地成了垃圾短信的受害者，消费者该到哪里说理去？

近日提交全国人大常委会审议的电子商务法草案，就给消费者提供了一个说理的地方，为信息安全的保护提供了法律依据。根据草案，第三方电商平台、平台内的经营者、支付服务提供者、快递物流服务提供者等都是信息安全保护责任主体。如果未履行保护义务，最高处50万元罚款并吊销执照；构成犯罪的，追究刑事责任。

没有金刚钻，别揽瓷器活。如果互联网服务提供商没有能力保护好用户的个人信息，那就不要染指。一旦收集了信息，就要尽最大努力，从技术上和管理上保护好。如果发生泄漏，就要依法承担法律责任，而非当事后诸葛，推卸责任。

当然，除了明确第三方平台的责任外，个人信息的保护也需多部门的联动，明确监管责任。同样需要相关法律规章的配套，将信息保护落到实处。

不起眼的广告短信和垃圾短信，背后其实是保护个人信息的大问题。什么时候广告短信也能多些真诚、少些套路，那我们才能真正地放心去买。

新华社发

他山之石

日本　立法先行，保护隐私

日本发生消费者信息遭到泄露、盗用事件的频率相对比较低。日本政府制订了一系列保护个人信息安全的法律，将民间企业也纳入个人信息保护的调整范围内。2002年，日本实施居民基本登记册上网制度。为使每个市民都能放心地享受互联网社会的便利，日本政府向国会提交了关于保护信息的5部法律。

其中，最重要的是《个人信息保护法》，这是日本保护个人信息安全的根本法律。该法2005年4月1日开始全面实施，特别规定在获得个人信息的时候，必须明确告知本人如何利用个人信息。此后，拥有个人信息的企业都被视为信息处理机构，需要向主管大臣报告有关情况，如果没有根据新法律采取有效的改善措施，将受到刑事处罚。由于《个人信息保护法》等条例的推广实施，不随便使用、泄露个人信息，已经成为日本人的一般性常识。任何组织在使用个人信息之前，都必须要和本人签署合约，限定信息使用的时间、空间范围，甚至到期时的处分方式。

美国　行业自律，立法保障

美国的行业自律模式主要有两种：一是建议性的行业指引，一般是行业组织、公司或产业实体制定该行业的行为指引或隐私标准，为行业内的隐私保护提供示范。二是网络隐私认证计划，该计划要求那些被许可在网站上张贴隐私认证标志的网站必须遵守在线资料收集的行为规则，并且服从多种形式的监督管理。

此外，针对信息安全事故的增多，美国也颁布相关法律保护信息安全，如《信息自由法》规范了第三方对包含个人信息的政府记录的获取；《电子通讯隐私法》禁止所有个人、企业和未经授权的政府部门对通讯内容进行窃听；《金融服务现代化法案》规定了金融机构处理个人私密信息的方式；《电讯法》规定电讯经营者有保守客户财产信息秘密的义务。

德国　“信息自决权”保护隐私

早在电子化远未普及的1970年，德国黑森州就颁布了《数据保护法》，成为全球最早的保护公民个人信息安全的国内立法。7年后，德国联邦政府颁布了首部《联邦数据保护法》，在联邦层面对个人信息保护作出统一规范。此后，《联邦数据保护法》和各个州的数据保护法相互配合，全面保护德国公民个人信息和隐私。

与美国的行业自律不同，德国为个人信息的保护设置了内外双重的监督模式。内部监管，指公共机构或私人机构设置内部数据保护专员。而外部监管，是指在数据机构之外设置的国家监管组织。《联邦数据保护法》设置了联邦数据保护专员对公共机构的数据行为进行监督，同时相应设置了数据保护监督机构对私人机构的数据行为进行监督。

（本报记者　王萌整理）

【侵犯公民个人信息犯罪案例】

一、北京顾某等非法获取计算机信息系统数据案

2016年6月，北京公安机关网络安全保卫部门破获顾某非法获取计算机信息系统数据案。经查，自2016年1月起，顾某非法获取公民个人账号约10万组。

二、江苏淮安“K8社工库”侵犯公民个人信息案

2016年3月，江苏淮安公安机关网络安全保卫部门成功侦破一起侵犯公民个人信息案，抓获犯罪嫌疑人8名，捣毁国内最大的网络社工库“K8社工库”（www.k8sec.com），查获公民个人信息20亿条。

三、四川广元侵犯公民个人信息案

2016年6月，经过一年多的侦查，四川广元公安机关网络安全保卫部门成功侦破一起侵犯公民个人信息犯罪案，抓获犯罪嫌疑人35名，查获四川全省学生信息及家长的公民个人信息1200万条，打掉非法买卖学生信息牟利的犯罪利益链条6个。

四、福建泉州“浮云网”侵犯公民个人信息案

2016年8月，福建泉州公安机关网络安全保卫部门破获“浮云网”侵犯公民个人信息案，抓获犯罪嫌疑人51人，成功打掉买卖公民个人信息的网站“浮云网”，查获公民个人信息2200万余条。

五、山东淄博侵犯公民个人信息案

2016年6月，山东淄博公安机关网络安全保卫部门破获一起侵犯公民个人信息案，抓获犯罪嫌疑人6名，打掉侵犯公民个人信息的犯罪源头2个，查扣公民个人信息近亿条。

六、江苏徐州非法获取计算机信息系统数据案

2016年6月，江苏徐州公安机关网络安全保卫部门破获一起非法获取计算机信息系统数据案，抓获犯罪嫌疑人8名，摧毁一条以黑客和快递公司内部员工为泄露源头的倒卖快递信息的黑色产业链，查扣各类快递信息500余万条，犯罪嫌疑人非法获利30余万元。

（来源：公安部官网）