安杰视点 | 严厉打击个人信息犯罪！改写大数据产业规则？

——简评《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》

前言

2016、2017 年我国在个人信息保护和网络安全领域的新立法可谓目不暇接。在行政法领域，继 2016 年 11 月《网络安全法》颁布后， 2017 年虽未过半，我们已经见到了《个人信息和重要数据出境安全评估办法（征求意见稿）》（4 月 11 日发布）和《网络产品和服务安全审查办法（试行）》（5 月 2 日发布）这两个重要的《网络安全法》配套规定。随着《网络安全法》于 6 月 1 日正式实施，包括关键信息基础设施分类和保护规定在内的其他配套规定和相关标准也将陆续出台；在民法领域，《民法总则》（3 月 15 日发布）首次将个人信息权利明确为公民的一项民事权利；而在刑法领域，最高人民法院和最高人民检察院也与时俱进，于 5 月 9 日公布了《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》（“两高解释”），对个人信息犯罪相关的刑法规定进行新形势下的诠释。此次两高解释所针对的是刑法第二百五十三条之一规定的“侵犯公民个人信息罪”、第二百八十七条之一规定的“非法利用信息网络罪”和第二百八十六条之一规定的“拒不履行信息网络安全管理义务罪”在刑法领域中的司法适用。

1. 扩大了个人信息的认定范围

对于何谓“个人信息”，在《网络安全法》颁布前已有的法律法规和司法解释可谓自行其是、各说各话，例如：

- 《电信和互联网用户个人信息保护规定》第四条规定：本规定所称用户个人信息，是指电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的**用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码**等能够单独或者与其他信息结合识别用户的信息**以及用户使用服务的时间、地点等信息**。
- 《侵害消费者权益行为处罚办法》第十一条规定：消费者个人信息是指经营者在提供商品或者服务活动中收集的**消费者姓名、性别、职业、出生日期、身份证件号码、住址、联系方式、收入和财产状况、健康状况、消费情况**等能够单独或者与其他信息结合识别消费者的信息。
- 《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》规定“网络用户或者网络服务提供者利用网络公开自然人**基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动**等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持。
- 《全国民事审判工作会议纪要》第 20 条规定：能够单独或者相互结合识别特定个人身份及行为隐私的信息构成网络公民个人信息(如网络用户的**网络认证账户和密码、IP 地址、上下线时间、网络浏览日志、网页地址、使用**

的搜索引擎关键词，公民个人的姓名、职业、家庭、婚姻、指纹、音频、视频等)。

上述各定义基本上均认同个人信息应包括“能够单独或者与其他信息结合识别自然人个人身份的信息”，但其列举的此类信息的具体类型不尽相同，个别信息类型是否能够达到“识别自然人个人身份”的标准尚有疑问；除此之外，上述定义还纳入了一些虽不具有“识别自然人个人身份”功能、但又具有某种隐私或私密属性的信息类型，例如“用户使用服务的时间、地点”、“网络浏览日志”、“网页地址”、“搜索引擎关键词”等。对“个人信息”定义的不一致，导致企业在商业运营中的认识混乱。

《网络安全法》对“个人信息”则采取了更为严格的判断标准，其第七十六条规定：“**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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等**。”该定义谨慎地将“能够单独或者与其他信息结合识别自然人个人身份”作为唯一的判断标准，其列举的个人信息类型均为公认可识别自然人身份的信息；该定义也没有纳入其他虽不具有“识别自然人个人身份”功能、但又具有某种隐私或私密属性的信息类型。这种定义方式更为克制，也有望统一个人信息的定义。

但此次两高解释将“公民个人信息”解释为:“**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，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等**。”该定义又一次将个人信息的定义覆盖到虽不具有“识别自然人个人身份”功能、但又具有某种隐私或私密属性的信息类型。而“反映特定自然人活动情况的信息”、“行踪轨迹”是否必定具有个人信息属性，或退一步讲是否必定具有隐私属性，也值得商榷。值得注意的是，虽然该定义与《网络安全法》中的定义不一致，但与最高院、最高检此前的司法解释可谓一脉相承。例如，2013年的《最高人民法院、最高人民检察院、公安部关于依法惩处侵害公民个人信息犯罪活动的通知》中规定：“公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份**或者涉及公民个人隐私的信息、数据资料**。”司法领域（两高解释）与立法领域（网络安全法）对个人信息定义的差异值得特别关注。

科学界定“个人信息”的内涵和外延的重要性在于，我国现有法律法规对于个人信息的收集和使用均以信息主体（即特定的自然人）的知情和同意为前提，未告知信息主体并取得其同意而收集、使用其信息即为非法。而两高解释将个人信息概念涵盖至“反映特定自然人活动情况的信息”和“行踪轨迹”等可能涉及公民个人隐私的信息，则扩大了适用知情同意原则的信息类型范围。对具有隐私属性的信息进行法律保护当然有必要，但笼统将此类信息作为个人信息处理，则增加了企业践行知情同意原则的难度和合规负担，并有可能导致司法实践中过度使用刑罚。实际上，对于何谓“隐私”在我国法律中也并无统一规定，根据相关判例中的表述，隐私一般指公民在生活中不愿公开、不愿为他人知悉的秘密。“反映特定自然人

活动情况的信息”和“行踪轨迹”是否能够满足“隐私”所要求的法律条件，恐怕也只能具体情况具体分析，笼统将其纳入个人信息的保护范畴值得商榷。

此外，上述定义看起来还将改写著名的 Cookie 技术与隐私权纠纷第一案[i]所确立的对我国大数据产业至关重要的规则，即不具有识别用户身份的个人网络活动轨迹及上网偏好不属于个人信息[ii]。依据该规则，企业似乎可在未经用户同意的情况下收集不具有识别用户身份的个人网络活动轨迹及上网偏好信息[iii]。使用 Cookie 或类似技术收集个人网络踪迹和偏好用于对用户进行“画像”和精准营销是大数据产业最普遍的应用之一，完全禁止使用此类技术并不现实。在两高解释发布之后，可以预见很多企业将尽可能扩大其隐私保护政策涵盖的用户个人信息的类别和使用方式（包括收集和使用 Cookie 或类似信息），从而满足用户“知情”和“同意”的要求。而对于有些与用户并无直接交互场景（例如没有网站或 App）、无法向用户公布或让用户同意其隐私政策的企业，践行用户知情同意原则较为困难，但如果继续收集、使用可识别个人身份的信息、或收集不具有识别用户身份的个人网络活动轨迹及上网偏好信息，则将面临较大的刑法风险。

2. 明确了“提供”公民个人信息的含义

在刑法第二百五十三条“侵犯公民个人信息罪”的条文中，对于何谓非法“提供”公民个人信息并无明确解释。此次两高解释明确了“提供”的含义。最高人民法院研究室主任颜茂昆在发布会上指出，对于“提供”行为应基于“举轻明重”的法理来认定。向特定人提供公民个人信息的行为属于“提供”，而通过信息网络或者其他途径予以发布，实际是向不特定多数人提供公民个人信息，更应当认定为“提供”。对此两高解释规定：“向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的，应当认定为刑法第二百五十三条之一规定的‘提供公民个人信息’。”

对于合法收集公民个人信息后非法提供的情形，两高解释规定：“未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的‘提供公民个人信息’，但是经过处理无法识别特定个人且不能复原的除外。“此次两高解释对于向他人提供公民个人信息的处理原则，与《网络安全法》保持一致[iv]，即被收集者的知情同意或数据匿名化（去可识别化）处理二者择一。

3. 扩大了非法利用信息网络罪适用范围

两高解释第八条规定：“设立用于实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组，情节严重的，应当依照刑法第二百八十七条之一的规定[v]，以非法利用信息网络罪定罪处罚；同时构成侵犯公民个人信息罪的，依照侵犯公民个人信息罪定罪处罚。“此举加大了针对个人信息犯罪的打击力度，将个人信息交易的网站、微信群、QQ 群等形式也明确纳入刑法打击范围。

4. 明确了网络服务提供者违反信息网络安全管理义务的刑事责任

网络服务提供者通常掌握大量用户个人信息，这些信息一旦泄露将可能造成恶劣社会影响和严重危害后果。对此，《网络安全法》明确了网络信息安全的责任主体，确立了“谁收集，谁负责”的基本原则[vi]。此次两高解释第九条规定：“网络服务提供者拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户的公民个人信息泄露，造成严重后果的，应当依照刑法第二百八十六条之一[vii]的规定，以拒不履行信息网络安全管理义务罪定罪处罚。“此举将有助于促使网络服务提供者更严格履行个人信息安全保护义务。

5. 明确了侵犯公民个人信息罪的定罪量刑标准

侵犯公民个人信息罪的入罪要件为“情节严重”。此次两高解释第五条第一款提出十项可认定为“情节严重”的情形，主要涉及信息类型和数量、违法所得数额、信息用途、主体身份、前科情况五个方面。两高解释第五条第二款对“情节特别严重”的适用标准亦作了明确，主要涉及是数量数额标准及造成严重后果两个方面。同时，两高解释明确了侵犯公民个人信息犯罪认罪认罚从宽处理规则：“实施侵犯公民个人信息犯罪，不属于‘情节特别严重’，行为人系初犯，全部退赃，并确有悔罪表现的，可以认定为情节轻微，不起诉或者免予刑事处罚；确有必要判处刑罚的，应当从宽处罚。”在司法实践中，行为人实施该类犯罪多是为牟取非法利益，基于此，两高解释同时明确了侵犯公民个人信息犯罪的罚金刑适用规则：“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一倍以上五倍以下。”具体内容可见下表：

<table>
<tr><th colspan="3">侵犯公民个人信息罪</th></tr>
<tr><th>刑法第二百五十三条之一</th><th colspan="2">两高解释</th></tr>
<tr><td rowspan="3">违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。
违反国家有关规定，将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的，依照前款的规定从重处罚。</td><td>“违反国家有关规定”</td><td>第二条违反法律、行政法规、部门规章有关公民个人信息保护的规定的。</td></tr>
<tr><td>“提供公民个人信息”</td><td>第三条向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的；未经被收集者同意，将合法收集的公民个人信息向他人提供的，但是经过处理无法识别特定个人且不能复原的除外。</td></tr>
<tr><td>“情节严重”</td><td>第五条非法获取、出售或者提供公民个人信息，具有下列情形之一的：

（一）出售或者提供行踪轨迹信息，被他人用于犯罪的；
（二）知道或者应当知道他人利用</td></tr>
</table>

		公民个人信息实施犯罪，向其出售或者提供的； （三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的； （四）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五百条以上的； （五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的； （六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的； （七）违法所得五千元以上的； （八）将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，数量或者数额达到第三项至第七项规定标准一半以上的； （九）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法获取、出售或者提供公民个人信息的； （十）其他情节严重的情形。 第六条为合法经营活动而非法购买、收受本解释第五条第一款第三项、第四项规定以外的公民个人信息，具有下列情形之一的： （一）利用非法购买、收受的公民个人信息获利五万元以上的； （二）曾因侵犯公民个人信息受过刑事处罚或者二年内受过行政处罚，又非法购买、收受公民个人信息的； （三）其他情节严重的情形。 实施前款规定的行为，将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准适用本解释第五条的规定。

	“情节特别严重”	实施第五条第一款规定的行为，具有下列情形之一的，应当认定为“情节特别严重”： （一）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的； （二）造成重大经济损失或者恶劣社会影响的； （三）数量或者数额达到前款第三项至第八项规定标准十倍以上的； （四）其他情节特别严重的情形。
窃取或者**以其他方法非法获取公民个人信息**的，依照第一款的规定处罚。	“以其他方法非法获取公民个人信息”	第四条违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的。
单位犯前三款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照各该款的规定处罚。	单位犯罪	第七条单位犯刑法第二百五十三条之一规定之罪的，依照本解释规定的相应自然人犯罪的定罪量刑标准，对直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

6. 明确了涉案公民个人信息的数量计算规则

结合司法实践中个人信息数量“计算难”的实际问题，两高解释第十一条专门规定了数量计算规则。最高人民法院研究室主任颜茂昆在发布会上指出：一是公民个人信息的条数计算：“非法获取公民个人信息后又出售或者提供的，公民个人信息的条数不重复计算”、“向不同单位或者个人分别出售、提供同一公民个人信息的，公民个人信息的条数累计计算”；二是对批量公民个人信息的数量认定：“对批量公民个人信息的条数，根据查获的数量直接认定，但是有证据证明信息不真实或者重复的除外。”

7. 结语

2016、2017 可谓网络安全和个人信息保护法律制度建设的“大年”。临近《网络安全法》正式实施，各项行政、民事和刑事配套法律法规和司法解释的密集颁布，对企业提出更严格的网络安全和个人信息保护要求。两高解释在我国刑法及《网络安全法》的基础上进一步明确并加强对个人信息犯罪的惩处力度，也将对中国互联网和数据产业乃至全社会产生深刻影响。**我们认为，相关企业有必要尽快“摸清家底”、充分掌握企业对内和对外关系中涉及网络安全、个人信息保护、重要数据保护的业务场景和合规需求，从而发现不足，并在此基础上建立和完善相**

关管理制度、流程和法律文件，以满足日益严格的法律要求。

我们将继续关注这一领域的进展并及时进行解读。

杨洪泉律师是安杰律师事务所合伙人，他在电信、互联网和IT（TMT）、争议解决、劳动等领域有丰富经验，尤为擅长提供个人信息保护和网络安全领域的法律服务。

---

[i]南京市中级人民法院，朱烨诉北京百度网讯科技公司隐私权纠纷案（2014）宁民终字第5028号

[ii]南京市中级人民法院对“北京百度网讯科技公司与朱烨隐私权纠纷案”作出的终审判决指出：“百度网讯公司在提供个性化推荐服务中运用网络技术收集、利用的是未能与网络用户个人身份对应识别的数据信息，该数据信息的匿名化特征不符合“个人信息”的可识别性要求……网络用户通过使用搜索引擎形成的检索关键词记录，虽然反映了网络用户的网络活动轨迹及上网偏好，具有隐私属性，但这种网络活动轨迹及上网偏好一旦与网络用户身份相分离，便无法确定具体的信息归属主体，不再属于个人信息范畴。”

[iii]在该案中，南京市中级人民法院认为百度网讯公司通过其《使用百度前必读》在对用户匿名信息进行收集、利用时采取了明示告知和默示同意相结合的方式。

[iv]《网络安全法》第四十二条第一款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。但是，经过处理无法识别特定个人且不能复原的除外。

[v]《中华人民共和国刑法》第二百八十七之一利用信息网络实施下列行为之一，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金：

（一）设立用于实施诈骗、传授犯罪方法、制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组的；

（二）发布有关制作或者销售毒品、枪支、淫秽物品等违禁物品、管制物品或者其他违法犯罪信息的；

（三）为实施诈骗等违法犯罪活动发布信息的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照第一款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

[vi]《网络安全法》第四十条规定：“网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。”

[vii]《刑法》第二百八十六条规定：网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

（一）致使违法信息大量传播的；

（二）致使用户信息泄露，造成严重后果的；

（三）致使刑事案件证据灭失，情节严重的；

（四）有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。