最高法、最高检官方解读《侵犯公民个人信息犯罪司法解释》

2017-05-11 [刑事实务](https://mp.weixin.qq.com/s?__biz=MzA3MTcwNDIyNw==&mid=2650599237&idx=2&sn=0b2358aa216599f1eca55e801bcc0247&chksm=8721c489b0564d9f0c5215ea958e84975bd547974ae3173f2314b042f596998a6bb482c0b7f1&scene=27&key=fa89a07420f7b4e69b43eaa049170f24b7af8e56c7eecf364aa3d1a4f7b2479e59ca0b241db41926f43c4ff0139142188bc0419cca39649a97e57838f43c1f0180d258d7a70a7c382a42652f5799da75&ascene=7&uin=MTkxMTU4MzAwOQ%3D%3D&devicetype=Windows+7&version=6203005d&pass_ticket=0a7xIZg%2BVgsN6%2FIiw9OyggtlXfPP3t2zUsN5HsxR%2ByJuks8rEKppURuyalZcCX6B&winzoom=1##)

《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》的理解与适用

日前，最高人民法院、最高人民检察院发布《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》（法释〔2017〕10号，以下简称《解释》），自2017年6月1日起施行。《解释》的公布施行，对于强化公民个人信息的刑事保护，维护个人信息安全和其他合法权益，必将发挥重要作用。为便于司法实践中正确理解和适用，现就《解释》的制定背景、起草中的主要考虑和主要内容介绍如下。

**一、《解释》的制定背景与经过**

随着信息化建设的推进，信息资源成为重要的生产要素和社会财富。而在各类信息中，个人信息的价值日益凸显，成为数字经济最重要的元素之一。与之同时，个人信息泄露问题严重，个人信息安全成为一个全社会高度关注的问题。为保护公民个人信息，2009年2月28日起施行的《刑法修正案（七）》增设了刑法第二百五十三条之一，规定了出售、非法提供公民个人信息罪和非法获取公民个人信息罪。《刑法修正案（七）》施行以来，各级公检法机关正确适用法律，准确认定事实，坚决依法惩处侵犯公民个人信息犯罪活动。2009年2月至2015年10月，全国法院新收出售、非法提供公民个人信息、非法获取公民个人信息刑事案件988起，审结969起，生效判决人数1415人。其中，新收出售、非法提供公民个人信息刑事案件101件，审结98件，生效判决人数142人；新收非法获取公民个人信息刑事案件887件，审结871件，生效判决人数1273人。

近年来，侵犯公民个人信息犯罪仍处于高发态势，不仅严重危害公民个人信息安全，而且与电信网络诈骗等犯罪存在密切关联，甚至与绑架、敲诈勒索等犯罪活动相结合，社会危害日益突出。为切实加大对公民个人信息的刑法保护力度，《刑法修正案（九）》对刑法第二百五十三条之一作出修改完善：一是扩大犯罪主体的范围，规定任何单位和个人违反国家有关规定，获取、出售或者提供公民个人信息，情节严重的，都构成犯罪；二是明确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，从重处罚；三是提升法定刑配置水平，增加规定“处三年以上七年以下有期徒刑，并处罚金”。修改后，“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”被整合为“侵犯公民个人信息罪”。《刑法修正案（九）》施行以来，各级公检法机关依据修改后刑法的规定，继续保持对侵犯公民个人信息犯罪的高压态势，实现案件量显著增长。2015年11月至2016年12月，全国法院新收侵犯公民个人信息刑事案件（含出售、非法提供公民个人信息、非法获取公民个人信息刑事案件）495件，审结464件，生效判决人数697人。

与此同时，司法实践反映，侵犯公民个人信息罪的具体定罪量刑标准尚不明确，一些法律适用问题存在争议，需要通过司法解释作出规定。为确保法律准确、统一适用，依法严厉惩治、有效防范侵犯公民个人信息犯罪，最高人民法院会同最高人民检察院，在公安部等有关部门的大力支持下，经深入调查研究、广泛征求意见，起草了《解释》。2017年3月20日最高人民法院审判委员会第1712次会议、2017年4月26日最高人民检察院第十二届检察委员会第63次会议审议通过了《解释》。

**二、《解释》起草中的主要考虑**

为确保《解释》的内容科学合理，能够适应形势发展、满足实践需要，在起草过程中，着重注意把握了以下几点：

**第一，贯彻刑法修改精神，强化对公民个人信息的刑法保护。**当前，侵犯公民个人信息犯罪呈高发多发态势，涉及的个人信息数量越来越大、类型越来越多。特别是，不少涉案公民个人信息事关他人财产乃至人身安全，如行踪轨迹、财产信息等敏感信息。基于当前侵犯公民个人信息犯罪的态势，根据修法精神，《解释》相关条文彰显了对侵犯公民个人信息犯罪的严惩立场，以加强对公民个人信息的刑法保护，有效维护公民的人身、财产安全和生活安宁。

**第二，坚持问题导向，有效解决司法实务问题。**从调研情况来看，对侵犯公民个人信息犯罪尚存在不少争议问题，亟需通过司法解释加以明确。例如，“公民个人信息”的内涵与外延，“出售或者提供公民个人信息”“非法获取公民个人信息”的理解，“情节严重”“情节特别严重”的把握，等等。基于此，《解释》相关条文以办理侵犯公民个人信息刑事案件存在的问题为基础，结合司法实际，作了明确规定。

**第三，坚持安全与发展并重，兼顾个人信息保护与大数据发展的需要。**在全球信息化快速发展的大背景下，大数据已成为国家重要的基础性战略资源，正引领新一轮科技创新。在大数据和云计算时代，包括个人信息在内的数据，只有充分地流动、共享、交易，才能实现集聚与规模效应，最大程度地发挥价值。但是，在数据流动、交易过程中如何保护公民个人信息的安全，避免个人信息扩散失控，也是必须面对的问题。实际上，公民个人信息的保护与大数据发展和信息社会的建设并不矛盾，二者之间的平衡点就在现行法律框架。质言之，大数据的发展应依法进行，信息社会须建立在依法保护个人信息的基础上，只有包括个人信息在内的数据在法律保护下安全迅速地收集和流通，才能真正推动我国信息产业的发展。因此，《解释》在刑法和《网络安全法》确立的框架范围内，兼顾公民个人信息保护与大数据产业发展的关系，确保在公民个人信息安全的前提下为大数据发展和信息化建设提供有力刑事司法保护。

**三、《解释》的主要内容**

《解释》结合当前侵犯公民个人信息犯罪的特点和司法实践反映的问题，依照刑法、刑事诉讼法的规定，对侵犯公民个人信息罪的定罪量刑标准和相关法律适用问题作了全面、系统的规定。《解释》共十三个条文，大致可以归纳为如下十个方面的问题：

**（一）“公民个人信息”的范围**

目前，我国关于个人信息的界定，最为权威的当属《网络安全法》的规定。《网络安全法》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。” 经研究认为，《网络安全法》将“个人信息”界定为“能够识别自然人个人身份的各种信息”，显然使用的是广义的“身份识别信息”的概念，即既包括狭义的身份识别信息（能够识别出特定自然人身份的信息），也包括体现特定自然人活动情况的信息。例如，从实践来看，行踪轨迹信息系事关人身安全的高度敏感信息，无疑应纳入法律保护范围，且应当重点保护。但是，行踪轨迹信息明显难以纳入狭义的“身份识别信息”的范畴。如果认为《网络安全法》将此类信息排除在“个人信息”的范围外，恐难以为一般人所认同，也不符合保护公民个人信息的立法精神。合理的解释应当是，《网络安全法》是广义上使用“身份识别信息”这一概念，亦即也包括个人活动情况信息在内。基于此，《解释》第一条在上述规定的基础上，进一步明确“公民个人信息”包括身份识别信息和活动情况信息，规定：“刑法第二百五十三条之一规定的‘公民个人信息’,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。”

此外，根据《解释》第一条的规定，关于“公民个人信息”的外延，有以下几个具体问题值得注意：（1）“公民个人信息”，既包括中国公民的个人信息，也包括外国公民和其他无国籍人的个人信息。（2）公民个人信息须与特定自然人关联。这是公民个人信息所具有的关键属性。因此，经过处理无法识别特定个人且不能复原的信息，虽然也可能反映自然人活动情况，但与特定自然人无直接关联，不能成为公民个人信息的范畴。对于与特定自然人关联，可以是识别特定自然人身份，也可以是反映特定自然人活动情况。需要注意的是，无论是识别特定自然人身份，还是反映特定自然人活动情况，都应当是能够单独或者与其他信息结合所具有的功能。例如，身份证号与公民个人身份一一对应，可以单独识别公民个人身份；而工作单位、家庭住址等无法单独识别公民个人身份，需要同其他信息结合才能识别公民个人身份。但是，上述两类信息无疑都属于公民个人信息的范畴。（3）与特定自然人关联的账号密码属于“公民个人信息”。对于“账号密码”能否纳入“公民个人信息”的范围，存在不同认识。经研究认为，当前账号密码往往绑定身份证号、手机号码等特定信息，即使未绑定，非法获取账号密码后往往也会引发侵犯财产甚至人身的违法犯罪。因此，《解释》第一条明确将“账号密码”列为“公民个人信息”的范围。

**（二）“违反国家有关规定”的认定**

《刑法修正案（九）》将侵犯公民个人信息罪的前提要件由“违反国家规定”修改为“违反国家有关规定”。根据修法精神，《解释》第二条规定：“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，应当认定为刑法第二百五十三条之一规定的‘违反国家有关规定’。”具体而言，该条将 “国家有关规定”明确限于法律、行政法规、部门规章等国家层面的规定，不包括地方性法规等非国家层面的规定。

**（三）非法“提供公民个人信息”的认定**

根据刑法第二百五十三条之一第一款、第二款的规定，违反国家有关规定，向他人非法出售或者提供公民个人信息，是侵犯公民个人信息罪的客观行为方式之一。从司法适用的角度，以下两个问题值得关注：

1.“提供”的认定。向特定人提供公民个人信息，属于“提供”公民个人信息，对此不存在疑义。但是，对于通过信息网络或者其他途径发布公民个人信息，是否属于“提供公民个人信息”，存在不同认识。经研究认为，通过信息网络或者其他途径发布公民个人信息，实际是向不特定多数人提供公民个人信息，向特定人提供公民个人信息的行为属于“提供”，基于“举轻明重”的法理，前者更应当认定为“提供”。基于此，《解释》第三条第一款规定：“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’。”

2.合法收集公民个人信息后非法提供的认定。基于大数据发展的现实需要，《网络安全法》在法律层面为个人信息交易和流动留有一定空间，第四十四条规定任何个人和组织“不得非法出售或者非法向他人提供个人信息”，即不仅允许合法提供公民个人信息，而且为合法出售公民个人信息留有空间。而且，《网络安全法》第四十二条第一款进一步明确了合法提供公民个人信息的情形，规定：“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。”据此，经得被收集者同意，以及匿名化处理（剔除个人关联），是合法提供公民个人信息的两种情形，不能纳入刑事规制范围。基于此，《解释》第三条第二款规定：“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。”当然，这里只是明确此种情形属于“提供公民个人信息”，是否构成侵犯公民个人信息罪，还需要根据“违反国家有关规定”等要件作进一步判断。

**（四）“非法获取公民个人信息”的认定**

根据刑法第二百五十三条之一第三款的规定，窃取或者以其他方法非法获取公民个人信息是侵犯公民个人信息罪的客观行为方式之一。具体而言，以下几个问题值得关注：

1.购买公民个人信息的处理。从实践来看，非法获取公民个人信息的方式主要表现为购买、收受、交换和侵入计算机信息系统或者采用其他技术手段。对于“购买公民个人信息”是否属于“以其他方法非法获取公民个人信息”，存在不同认识。有意见认为，“其他方法”应当限于与“窃取”危害性相当的方式（如抢夺），不宜将“购买”包括在内。经研究认为，其一，刑法第二百五十三条之一第三款并未明确排除“购买”方法，且非法购买公民个人信息当然属于非法获取公民个人信息的情形。其二，从实践来看，当前非法获取公民个人信息的方式主要表现为非法购买，如排除此种方式，则会大幅限缩侵犯公民个人信息罪的适用范围。其三，不少侵犯公民个人信息犯罪案件，购买往往是后续出售、提供的前端环节，没有购买就没有后续的出售、提供。基于上述考虑，《解释》第四条明确规定：“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，属于刑法第二百五十三条之一第三款规定的‘以其他方法非法获取公民个人信息’。”

2.获取公民个人信息行为“非法”的判断。对于获取公民个人信息，刑法第二百五十三条之一第三款将罪状直接表述为“非法获取”。基于体系解释的原理，对此处的“非法”，应当以是否违反国家有关规定作为判断标准。

3.非法收集公民个人信息的处理。《网络安全法》第四十一条规定：“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。”“网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。”违反上述规定，未经他人同意收集公民个人信息，或者收集与提供的服务无关的公民个人信息的，应当认定为“非法获取公民个人信息”。以此为基础，《解释》第四条专门明确，违反国家有关规定，在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的“以其他方法非法获取公民个人信息”。

**（五）侵犯公民个人信息罪的**

定罪量刑标准

根据刑法第二百五十三条之一的规定，非法获取、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。可见，侵犯公民个人信息罪系情节犯，定罪量刑标准为“情节严重”“情节特别严重”。对于这一概括性的定罪量刑情节，宜根据司法实践的情况从犯罪的客体、客观方面、主体、主观方面等多个角度加以考察。经充分调研，《解释》第五条规定了“情节严重”“情节特别严重”的认定标准。

1.“情节严重”的认定标准。《解释》第五条第一款从以下几个方面对侵犯公民个人信息罪的入罪标准“情节严重”作了明确：

一是信息类型和数量。公民个人信息的类型繁多，行踪轨迹信息、通信内容、征信信息、财产信息、住宿信息、交易信息等公民个人敏感信息涉及人身安全和财产安全，被非法获取、出售或者提供后极易引发绑架、诈骗、敲诈勒索等关联犯罪，具有更大的社会危害性。因此，基于不同类型公民个人信息的重要程度，《解释》分别设置了“五十条以上”“五百条以上”“五千条以上”的入罪标准，以实现罪责刑相适应。具体而言：

（1）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。行踪轨迹信息、通信内容、征信信息、财产信息与人身安全、财产安全直接相关，系高度敏感信息，《解释》第五条第一款第三项将入罪标准设置为“五十条以上”。需要注意的是，鉴于本项规定的入罪标准门槛较低，故此处严格限缩所涉公民个人信息的类型，仅限于行踪轨迹信息、通信内容、征信信息、财产信息四类信息，不允许司法适用中再通过等外解释予以扩大。对于行踪轨迹信息、通信内容、征信信息，司法实践中在认定上不存在争议。对于财产信息，可以根据案件具体情况把握：既包括银行账户、第三方支付结算帐户、证券期货等金融服务账户的身份认证信息（一组确认用户操作权限的数据，包括账号、口令、密码、数字证书等），也包括存款、房产等财产状况信息。

（2）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。上述公民个人信息虽然在重要程度上弱于行踪轨迹信息、通信内容、征信信息、财产信息，但也与人身安全、财产安全直接相关，往往被用于“精准”诈骗等违法犯罪活动。基于此，《解释》第五条第一款第四项将入罪标准设置为“五百条以上”。需要注意的是，本项规定有“等其他可能影响人身、财产安全的公民个人信息”的表述，司法实践中可以根据具体情况作等外解释，但应当确保所适用的公民个人信息涉及人身、财产安全，且与“住宿信息、通信记录、健康生理信息、交易信息”在重要程度上具有相当性。

（3）非法获取、出售或者提供一般公民个人信息五千条以上的。从实践来看，除前述公民个人敏感信息外，出售、提供公民个人信息往往数量较大，动辄数万条甚至数十万条，在不少案件中甚至将公民个人信息编辑为电子文档后按兆出售。因此，不少地方对出售、提供公民个人信息的入罪掌握在数量五千条以上，基本上可以满足严厉打击此类犯罪的需要，且给行政处罚留有一定空间。基于此，《解释》第五条第一款第五项设置较低的入罪标准，将非法获取、出售或者提供公民个人信息五千条以上的规定为“情节严重”。

此外，鉴于实践中存在混杂公民个人信息的情形，《解释》第五条第一款第六项将“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”情形规定为“情节严重”。

二是违法所得数额。出售或者非法提供公民个人信息往往是为了牟利，故应当以违法所得作为认定“情节严重”的情形之一。从司法实践来看，一般公民个人信息的价格相对较低，甚至不会按条计价；而公民个人敏感信息价格通常较高，通常按条计价，特别是行踪轨迹信息可以谓之为最为昂贵的信息类型。考虑到各项规定之间的均衡，《解释》第五条第一款第七项将违法所得五千元以上的规定为“情节严重”。

三是信息用途。通常而言，非法获取公民个人信息，绝不仅是为了占有，而是有特定用途、甚至用于违法犯罪。可以说，非法获取、出售或者提供公民个人信息，不仅严重危害公民的信息安全，而且可能引发进一步犯罪。因此，此类行为引发的后果的严重程度，是认定“情节严重”与否的重要标准。被非法获取、出售或者提供的公民个人信息，用途存在不同，对权利人的侵害程度也会存在差异。如果涉案的公民个人信息被用于实施其他犯罪活动，使权利人的人身、财产安全陷入高风险状态或者造成实质危害的，对此应当直接认定为“情节严重”或者“情节特别严重”，以刑事手段加以规制；而如果涉案公民个人信息未被用于犯罪活动，则社会危害性相对较小，不宜直接以此作为刑事规制的依据。基于此，《解释》第五条第一款第二项将“知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的”规定为“情节严重”。从司法实践来看，行踪轨迹信息是最为敏感的公民个人信息。非法获取、出售或者提供该类信息，行为人主观上对可能被用于犯罪存在概括认识，《解释》第五条第一款第一项直接将“非法获取、出售或者提供行踪轨迹信息，被他人用于犯罪的”规定为“情节严重”，无须再具体判断主观上是否知道或者应当知道涉案信息被用于犯罪。

四是主体身份。公民个人信息泄露案件不少系内部人员作案，诸多公民个人信息买卖案件也可以见到“内鬼”参与的“影子”。这是侵犯公民个人信息违法犯罪泛滥的重要原因所在。由于上述情形往往发生在公民个人信息交易的最初阶段，涉案信息的数量往往较少、价格相对低廉。此种情形下，如果不设置特殊标准，往往难以对此类源头行为予以刑事惩治。基于此，为贯彻落实刑法第二百五十三条之一第二款“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”的规定，《解释》第五条第一款第八项对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情形认定为“情节严重”设置了特殊标准，规定此种情形下出售或者提供公民个人信息，认定“情节严重”的数量、数额标准减半计算。当然，对于此种情形，不宜再根据刑法第二百五十三条之一第二款的规定从重处罚，以免重复评价。

五是主观恶性。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，行为人屡罚屡犯，主观恶性大。故而，《解释》第五条第一款第九项将此种情形规定为“情节严重”。

2.“情节特别严重”的认定标准。《解释》第五条第二款主要从两个层面规定了“情节特别严重”的情形：一是数量数额标准。基于司法实践中侵犯公民个人信息犯罪涉案的公民个人信息数量相差悬殊，跨度从几千条到几十万条（甚至更大数量）不等，将“情节特别严重”和“情节严重”之间的数量数额标准设置为十倍而非五倍的倍数关系。二是严重后果。从实践来看，非法获取、出售或者提供公民个人信息，对于个人而言，可能造成人身伤亡、经济损失等后果；对于社会而言，可能引发社会恐慌，造成恶劣社会影响。基于此，将“造成被害人死亡、重伤、精神失常或者被绑架等严重后果的”“造成重大经济损失或者恶劣社会影响的”规定为“情节特别严重”。

3.为合法经营活动购买、收受公民个人信息定罪量刑的特殊标准。从实践来看，购买、收受公民个人信息从事广告推销等活动的情形较为普遍。为了秉持刑法的谦抑性，体现宽严相济，《解释》第六条第一款规定：“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，应当认定为刑法第二百五十三条之一规定的’情节严重’：（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。”这是《解释》针对为合法经营活动而购买、收受公民个人信息的行为设置的专门的定罪量刑标准。而且，考虑到此类行为社会危害性不大，即使构成犯罪，通常也不需要升档量刑，故只规定了“情节严重”的具体情形。

需要注意的是，适用该定罪量刑标准须满足三个条件：一是为了合法经营活动，对此可以综合全案证据认定，但主要应当由被告方提供相关证据；二是限于普通公民个人信息，即不包括可能影响人身、财产安全的敏感信息；三是信息没有再流出扩散，即行为方式限于购买、收受。根据《解释》第六条第二款的规定，如果将购买、收受的公民个人信息非法出售或者提供的，定罪量刑标准应当适用《解释》第五条的规定。对此应当注意的是，为了合法经营活动交换公民个人信息的，由于在获取信息的同时造成了信息扩散，不符合前述三个要件，定罪量刑标准亦应适用《解释》第五条的规定。

4.侵犯公民个人信息单位犯罪的定罪量刑标准。根据刑法第二百五十三条之一第四款的规定，单位可以成为侵犯公民个人信息罪的主体。为切实加大对单位侵犯公民个人信息犯罪的惩治力度，《解释》第七条明确了单位实施侵犯公民个人信息犯罪的，适用自然人犯罪的定罪量刑标准，规定：“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。”

**(六)侵犯公民个人信息罪的**

认罪认罚从宽处理

为贯彻落实“认罪认罚从宽制度”，充分发挥刑法的教育和威慑功能，《解释》第十条专门规定：“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。”可见，该条只适用于侵犯公民个人信息犯罪的基本情节，对于符合“情节特别严重”构成的，不能再适用本条规定从宽处罚。

**（七）设立网站、通讯群组**

侵犯公民个人信息行为的定性

实践中，一些行为人通过建立网站供他人进行公民个人信息交换、买卖等活动，以非法牟利。此类网站存储、流转公民个人信息量巨大，但网站建立者、直接负责的管理者未直接接触公民个人信息，不少情形下难以按照侵犯公民个人信息罪定罪处罚。根据刑法第二百八十七条之一的规定，设立用于实施违法犯罪活动的网站、通讯群组，情节严重的，构成非法利用信息网络罪。经研究认为，供他人实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组实际上属于“用于实施违法犯罪活动的网站、通讯群组”。因此，《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，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。

**（八）拒不履行公民个人信息**

安全管理义务行为的处理

当前，一些单位因为履行职责或者提供服务的需要，掌握着海量公民个人信息，这些信息一旦泄露将造成恶劣社会影响和严重危害后果。实际上，侵犯公民个人信息违法犯罪的猖獗，与有关单位保护公民个人信息工作存在疏漏有一定关联，相关管理机制有进一步完善的空间。这一问题在互联网时代更为突出。为了促进网络运营者采取切实有效的措施加强对公民个人信息的保护，《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”的原则，将收集和使用个人信息的网络运营者，设定为个人信息保护的责任主体。其中，第四十条明确规定：“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。”与之相衔接，《刑法修正案（九）》设立了拒不履行信息网络安全管理义务罪，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，致使用户信息泄露，造成严重后果的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金。因此，对于网络服务提供者未切实落实个人信息保护措施，符合刑法第二百八十六条之一规定的，可能构成拒不履行信息网络安全管理义务罪。据此，《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的规定，以拒不履行信息网络安全管理义务罪定罪处罚。”

**（九）涉案公民个人信息的数量计算规则**

针对公民个人信息数量“计算难”的实际问题，《解释》第十一条专门规定了数量计算规则。具体而言：

1.公民个人信息的条数计算。关于公民个人信息的条数计算，如同一条信息中涉及多个个人信息的，如家庭住址、银行卡信息、电话号码，实践中往往认定为一条公民个人信息。对此问题，实践中并无太大争议,故未作专门规定。对于实践中存在的针对同一对象非法获取公民信息后又出售或者提供的情形，则明显不宜先计算非法获取的公民个人信息数量、再计算出售或者提供的公民个人信息数量，故《解释》第十一条第一款规定：“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。”此外，考虑到公民个人信息可能被重复出售或者提供，其社会危害性明显不同于向他人出售或者提供一次的情形，故而，《解释》第十一条第二款规定：“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。”

2.批量公民个人信息的数量认定规则。从实践来看，除公民个人敏感信息外，涉案的公民个人信息动辄上万条甚至数十万条。此类案件中，不排除少数情况下存在信息重复，如针对同一对象并存“姓名+住址”“姓名+电话号码”“姓名+身份证号”等数条信息，但要求做到完全去重较为困难。此外，对于信息的真实性也难以一一核实。个别案件中，要求办案机关电话联系权利人核实公民个人信息的做法，明显不合适。基于此，《解释》第十一条第三款规定：“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。”

**（十）侵犯公民个人信息犯罪的**

罚金刑适用规则

侵犯公民个人信息犯罪具有明显的牟利性，行为人实施该类犯罪主要是为了牟取非法利益。因此，有必要加大财产刑的适用力度，让行为人在经济上得不偿失，进而剥夺其再次实施此类犯罪的经济能力。基于此，《解释》第十二条规定：“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。”

|  |
| --- |
| 降低入罪门槛，严惩侵犯公民个人信息犯罪——“两高”《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》解读《检察日报》侵犯公民个人信息罪入罪要件“情节严重”如何界定？拒不履行公民个人信息安全管理义务的行为是否担责？涉案公民个人信息的数量计算遵守怎样的规则？今天上午，最高人民法院、最高人民检察院联合召开新闻发布会，发布《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》（下称《解释》），对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定。最高法、最高检有关部门负责人就《解释》相关亮点在新闻发布会上回应了媒体关切。从五个角度准确认定“情节严重”侵犯公民个人信息罪的入罪要件为“情节严重”。最高法研究室主任颜茂昆介绍说，根据法律精神，结合司法实践，《解释》第五条第一款设十项对“情节严重”的认定标准作了明确规定，大致涉及如下五个方面：**一是信息类型和数量。**基于不同类型公民个人信息的重要程度，《解释》分别设置了“五十条以上”“五百条以上”“五千条以上”的入罪标准，以体现罪责刑相适应。**二是违法所得数额。**出售或者非法提供公民个人信息往往是为了牟利，基于此，《解释》将违法所得五千元以上的规定为“情节严重”。**三是信息用途。**《解释》将“非法获取、出售或者提供行踪轨迹信息，被他人用于犯罪”“知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供”规定为“情节严重”。**四是主体身份。**公民个人信息泄露案件不少系内部人员作案，对此，《解释》明确，“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，认定“情节严重”的数量、数额标准减半计算。**五是前科情况。**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，行为人屡教不改、主观恶性大，《解释》将其也规定为“情节严重”。设立网站侵犯个人信息可构成非法利用信息网络罪实践中，一些行为人建立网站、通讯群组供他人进行公民个人信息交换、流转、销售，以非法牟利。颜茂昆说，根据刑法有关规定，设立用于实施违法犯罪活动的网站、通讯群组，情节严重的，构成非法利用信息网络罪。供他人实施非法获取、出售或者提供公民个人信息违法犯罪活动的网站、通讯群组实际上属于“用于实施违法犯罪活动的网站、通讯群组”。对此，《解释》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，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。”拒不履行管理义务，网络运营者或触刑法当前，不少网络运营者因为履行职责或者提供服务的需要，掌握着海量公民个人信息，这些信息一旦泄露将造成恶劣社会影响和严重危害后果。对此，网络安全法明确规定：“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。”为进一步促使网络服务提供者切实履行个人信息安全保护义务，《解释》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的规定，以拒不履行信息网络安全管理义务罪定罪处罚。破解公民个人信息数量“计算难”公民个人信息数量是侵犯公民个人信息案件定罪量刑标准的主要依据，至关重要。实践中，司法机关查获的涉案信息数量动辄上万条、数十万条，甚至以兆计算，怎样科学、合理认定信息数量是办案部门一直难以解决的问题。新闻发布会上，最高检法律政策研究室副主任缐杰介绍说，为增强《解释》的可操作性，《解释》专门规定了数量计算规则。如《解释》规定：“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。” “非法获取了他人拨打电话的记录五十条，将其出售给同一人或者单位的，应当认定为侵犯公民个人信息五十条。”缐杰解释道。按照《解释》，公民个人信息向不同对象分别出售、提供的，属于重复出售或者提供个人信息，社会危害性较一次性出售或提供危害性更大，数量应累计计算。比如，非法获取了他人拨打电话的记录五十条，将其出售给两个人或者单位的，应当认定为侵犯公民个人信息一百条。针对涉案的公民个人信息上万条甚至更多的，可能存在信息重复的情况，《解释》特别规定：“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。” |

“说刑品案”公众号解读

一、立法沿革

1997年刑法大修时未作相关规定。针对侵犯公民个人信息犯罪日趋严重的趋势，2009年刑法修正案（七）在刑法第二百五十三条后新增了一条，作为第二百五十三条之一，共３款：（1）“国家机关或者金融、电信、交通、教育、医疗等单位的工作人员，违反国家规定，将本单位在履行职责或者提供服务过程中获得的公民个人信息，出售或者非法提供给他人，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”；（2）“窃取或者以其他方法非法获取上述信息，情节严重的，依照前款的规定处罚”；（3）“单位犯前两款罪的，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”。

最高人民法院、最高人民检察院将上述条款概括出了两个罪名：“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”。

2015年刑法修正案（九）对第二百五十三条之一作了修改，增至４款：（1）“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”；（2）“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”；（3）“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”；（4）“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”。

对照新旧条款可见，刑法修正案（九）扩大了犯罪主体的范围，对履行职责或者提供服务过程中实施的犯罪从重处罚，并加重法定刑，增加了“情节特别严重”情形下的法定刑档次等。“两高”的最新罪名解释将上述条款统一归为一个罪名：“侵犯公民个人信息罪”，“出售、非法提供公民个人信息罪”和“非法获取公民个人信息罪”两个罪名由此被取消。

二、行为对象

 “公民个人信息”的范围如何确定，是一个较为关键的问题。国内刑法理论界对此有关联说、隐私说和识别说等不同主张。关联说认为，凡是与个人存在关联的信息都属于个人信息，其外延十分广泛，几乎有关个人的一切信息、数据或者情况都可以被认定为个人信息。隐私说认为，只有与个人隐私相关的才属个人信息。识别说认为，公民个人信息是指姓名、职业、职务、年龄、婚姻状况、学历、专业资格等能够识别公民个人身份的信息。

从近些年各地判决情况看，涉及的范围比较广泛，既有身份信息、财产信息、交易信息，还有行踪信息、通话信息、教育信息等，几乎囊括了个人生活的各个方面。

相比较而言，关联说对个人信息的定义较为宽泛，其将所有与个人相关的信息都包含其中，容易造成犯罪打击面的扩大化，所以，赞同关联说并不被国内司法实务界所认同，目前主要分歧还在于“识别说”和“隐私说”。从司法解释的界定看，更多地是把“识别性”作为认定个人信息的核心属性。

 《解释》第１条规定：“公民个人信息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”。由此，将“公民个人信息”由身份识别信息扩至两大类：一是身份识别信息；二是活动情况信息。具体包括姓名、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，

三、行为方式

侵犯公民个人信息罪在客观方面表现为两种行为方式：

（一）违反国家有关规定，向他人出售或者提供公民个人信息

1．“违反国家有关规定”不同于“违反国家规定”，前者的范围更为宽泛。我国尚未制定专门的公民个人信息保护法，但一些专门的法律、法规对特定领域公民个人信息的保护有专门规定。所以，《解释》第2条规定：“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，应当认定为刑法第二百五十三条之一规定的‘违反国家有关规定’”。

2．此类行为又区分出“向他人出售或者提供公民个人信息”和“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”两种情形。后一种情形通常表现为“内鬼”犯罪，对此依法需要从重处罚。并且，在司法解释规定的入罪标准上“减半掌握”，涉案信息的数量或者数额达到法定标准一半就可定罪，从分体现了对“内鬼”的从严惩治。

3．关于“非法提供”，《解释》明确了两种情况：一是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（即将公民个信息提供给不特定的对象）。二是未经被收集者同意，将合法收集的公民个人信息向他人提供。该两种情况都属于“非法提供”。当然，后一种情形属于“合法收集、非法提供”，解释规定了例外情形，即经过处理无法识别特定个人且不能复原的，可不予认定。

（二）窃取或者以其他方法非法获取公民个人信息

 “窃取”是指采用秘密的或者不为人知的方法取得他人个人信息的行为。严格地讲，“窃取”也是“非法获取”的一种方式，只是由于窃取的方式较为常见，故法条将其独立规定。

这里需要重点把握“其他方法”。从立法用语上讲，它应指“窃取”以外的其他方法。《解释》明确了两种情形：一是违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息”。二是根据《网络安全法》规定的收集、使用个人信息的规则，明确违反国家有关规定，在履行职责、提供服务过程中收集公民个人信息。

四、情节严重

根据刑法第二百五十三条之一的规定，出售、非法提供公民个人信息，窃取或者非法获取公民个人信息，均以“情节严重”为入罪要件。如果未达到情节严重的程度，如系初犯，涉案公民个人信息数量较小、获利较少等，则不构成犯罪，可以根据具体情况予以行政处罚。

关于“情节严重”的具体认定标准，刑法未作具体规定，在以往的判决中，司法机关主要根据涉案信息的类型和数量，被告人获利情况、信息用途、危害后果及信息获取手段等因素综合判断，存在适用标准不统一的问题。

为此，《解释》作了细化规定，具体列举了以下10种非法获取、出售或者提供公民个人信息的情形，属于“情节严重”：

（1）出售或者提供行踪轨迹信息，被他人用于犯罪的；

（2）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；

（3）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；

（4）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；

（5）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；

（6）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；

（7）违法所得五千元以上的；

（8）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；

（9）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；

（10）其它情节严重的情形。

如果实施非法出售、获取或提供公民个人信息的行为，具备以下4种情况，则属于“情节特别严重”：

（1）造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；

（2）造成重大经济损失或者恶劣社会影响的；

（3）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；

（4）其他情节特别严重的情形。

针对为合法经营活动而非法购买、收受公民个人信息的特殊情况，《解释》规定，如果非法购买、收受行踪轨迹信息、通信内容、征信信息、财产信息、住宿信息、通信记录、健康生理信息、交易信息等敏感信息以外的信息的，予以特别考虑，即利用非法购买、收受的公民个人信息获利五万元以上的以及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，认定“情节严重”。但是，如果将购买、收受的公民个人信息非法出售或者提供的，则对其定罪量刑的标准“一视同仁”。

《解释》还注重贯彻宽严相济刑事政策，特别规定：“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，不起诉或者免于刑事处罚；确有必要判处刑罚的，应当从宽处罚。”需要注意的是，该条规定只适用于侵犯公民个人信息犯罪的基本情节，对于“情节特别严重”的排除适用。

此外，《解释》对信息数量的计算方法也予以明确：（1）“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”；（2）“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”；（3）“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。”同时提出：“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。”

五、“人肉搜索”

在“人肉搜索”案件中，行为人未经权利人同意即将其身份、照片、姓名、生活细节等个人信息公布于众，影响其正常的工作、生活秩序，危害严重。更有甚者，一些行为人恶意利用泄露的个人信息进行各类违法犯罪活动。所以，近年来社会上一直有将“人肉搜索”行为入罪的呼声。为此，《解释》第3条特别规定：“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’。”这就把“人肉搜索”直接纳入了刑法规制。

六、罪数问题

《解释》明确了两类行为的定性：一是设立网站、通讯群组侵犯公民个人信息行为的定性。《解释》第8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，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。”

二是拒不履行公民个人信息安全管理义务行为的处理。《解释》第9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的规定，以拒不履行信息网络安全管理义务罪定罪处罚。”

值得注意的是，《关于加强网络信息保护的决定》对公民个人电子信息的保护作了规定，违反规定非法获取公民个人电子信息的行为，无疑属于修正后刑法第二百五十三条之一规定的非法获取公民个人信息的行为。但是，公民个人电子信息往往表现为计算机信息系统数据，故非法获取公民个人电子信息的行为有时会同时触犯侵犯公民个人信息罪与非法获取计算机信息系统数据罪。对此如何处理，实践中认识有分歧。有一种主张认为，这种情况属于想象竞合犯，应从一重罪处罚。但如果按照刑法第第287条关于“利用计算机实施金融诈骗、盗窃、贪污、挪用公款、窃取国家秘密获取其它犯罪的，依照本法有关规定定罪处罚”的特别规定，此种情况似应以“侵犯公民个人信息罪”追究刑事责任。

七、十大判例

（一）刑事审判参考案例（3个）

1．周建平非法获取公民个人信息案（指导案例第612号）

［裁判要旨］：电话通话清单隐含着公民个人的某些信息，属于刑法第二百五十三条之一罪状中“公民个人信息”的范畴。非法购买公民电话清单后又出售牟利的，依法构成侵犯公民个人信息罪。

2．周娟等非法获取公民个人信息案（指导案例第719号）

［裁判要旨］：对公民个人信息未经授权的不当获取属于“非法获取”。是否入罪，不能唯数量论，即使涉案信息数量不大，但有其他严重情节的，也能够构成犯罪。

3．谢新冲出售公民个人信息案（指导案例第741号）

［裁判要旨］：手机定位信息属于刑法所保护的“公民个人信息”。

（二）其他案例（7个）

1．邵保明等侵犯公民个人信息案（浙江省东阳市人民法院判决）

［裁判要旨］：非法出售户籍信息、手机定位、住宿记录等个人信息，构成侵犯公民个人信息罪。

2．韩世杰、旷源鸿、韩文华等侵犯公民个人信息案（湖北省巴东县人民法院判决）

［裁判要旨］：非法查询征信信息牟利，构成侵犯公民个人信息罪。

3．周滨城等侵犯公民个人信息案（浙江省平湖市人民法院判决）

［裁判要旨］：非法购买学生信息出售牟利，构成侵犯公民个人信息罪。

4．夏拂晓侵犯公民个人信息案（浙江省绍兴市柯桥区人民法院判决）

［裁判要旨］：非法买卖网购订单信息，构成侵犯公民个人信息罪。

5．肖凡、周浩等侵犯公民个人信息案（内蒙古自治区赤峰市红山区人民法院判决）

［裁判要旨］利用黑客手段窃取公民个人信息出售牟利，构成侵犯公民个人信息罪。

6．杜明兴、杜明龙侵犯公民个人信息案（江苏省南京市鼓楼区人民法院判决）

［裁判要旨］通过互联网非法购买、交换、出售公民个人信息，构成侵犯公民个人信息罪。

7．丁亚光侵犯公民个人信息案（浙江省乐清市人民法院判决）

［裁判要旨］非法提供近二千万条住宿记录供他人查询牟利，构成侵犯公民个人信息罪“情节特别严重”。