

□屈学武/文 (作者系中国社会科学院法学研究所研究员)

# “特工 007” 行为性质解读及法律思考

## 一、“特工 007”行为简介

近来,在国内某交易网站上,有人特设了自己的“特工 007 专用产品”销售网页,题为“特工 007 专用产品一部手机同时拥有 16 个号码”。其中“商品描述”一栏中的开篇语为:“全球创新 GSM 手机号码 COPY 技术”;“……本卡是引进台湾技术的高科技产品,俗称‘1 卡 16 号’,可将不同的 16 只手机号码,中国移动(联通)130、131、135、137、138、139……所有的 GSM sim 卡都备份 COPY 至一张卡上”。

根据读者的举报,首都《京华时报》和中央电视台的记者先后通过该网站与“特工 007”取得了联系并购得了该“卡”,从而了解和证实了有关情况。原来,买家通过 280 元/件所购得的并非仅仅一张卡,而是“三件套”,包括:一台解码器、一套可复制(他人手机号码的)软件、一张可反复使用和擦写的空白可复制卡。

据报载,<sup>①</sup>有记者买到该“三件套”后,首先将其软件安装到了计算机中,而后按软件的提示,将一张从电信部门购得的 GSM 手机的正版智能 SIM 卡装入解码器进行扫描解码,历时 2 个多小时,进而再按照该软件的提示,取出正版的 SIM 卡,插入从“特工 007”处购得的可复制卡,这一回,仅只“瞬间”就完成了手

机 SIM 卡的复制工作。

这样一来,复制人就可将此非法复制的 SIM 卡插入任何适于 GSM 制式的裸机上,进而使用他人的手机号码与人通话,结果是被盗号人承担了全部通话费用。而且,按照该软件的“使用说明”,该“三件套”上的可复制空白卡,可一举复制并承载 16 个他人电话号码。与此同时,鉴于 GSM 制式的 SIM 卡可同时储存机主的通信簿,因而复制者在盗得他人电话号码的同时,也非法盗得了他人的通信簿资料。

经验证明,事实正如“特工 007 专用产品”功能介绍里所说的那样,复制后,原卡和烧卡(即非法盗取的码号)均可使用,效果无异。只是原卡和被盗号卡不能同时拨号通话;接听来话时,使用同一码号的两个手机不能同时接听。

据上文报道:该卖主在与假充“买主”的记者通话时声称:“买这种卡的主要就是一些有公款报销待遇的人,复制了之后可以将复制卡赠送给自己的亲友,话费由公款报销。此外,就是用来盗打他人电话”。该卖主还声称他们的产品在广州、东莞、上海等地卖的“特别火”,而“其他地方则处于半公开状态”。上海的销量很大,“基本上每天可以卖出 200 个”——由此“自白”可见,卖主自己也知道其所干之事非法,其产品才会其他地方“不能完全公开”

而是处于“半公开状态”。对此,国家信息产业部与北京移动通信公司相关管理部门都明确表示:此种做法违法。

## 二、“特工 007”行为性质解读

“特工 007”的违法性究竟何在呢?无疑,其行为少不了某些民事或经济违法性;但主要表现为刑事违法性,准确地说,“007”的网络内外销售活动,涉嫌一系列具有共犯(甚至犯罪集团)性质的连环违法犯罪活动。其活动流程大致如下:其一,网下批量非法生产其“产品”。按其广告宣称,产地在台湾,从而本案可能涉嫌跨境犯罪;其二,网上虚假广告宣传;其三,网络内外的非法经营;其四,网络内外传授犯罪方法;其五,教唆犯罪。其违法犯罪过程及其特征如下:

“特工 007”的第一环节活动是:批量非法生产其“产品”。这一活动的实质是共同侵犯商业秘密。对此,有人可能质疑:“特工 007”可能只销不产,如何能肯定该“007”与生产者共同行为人呢?回答是:“007”既然自称自己每天仅在上海就可以卖出 200 套产品,且其确实已在该网站上成交“产品”多日,由此可见,其并非“一次性”地售卖自己的旧物,而是在批量售出自己或他人生产的“产品”。这样一来,无论是“007”自产自销,还是他人产、“007”代销,从刑法

<sup>①</sup>详见 2003 年 6 月 9 日《京华时报》:《网上热卖手机卡复制器》一文。

的视角看,产销双方无疑已在销售之前,达成了共同实施此一系列活动的事前通谋,因而无论“007”是否生产者本身,都脱不了共同侵犯商业秘密的干系。

然而,生产上述三套件,又是如何与“商业秘密”关联上的呢?联结点在于:而今面世的每一台GSM制式手机内装的SIM卡,实际上都隐含着机密度极高的内置密码。每张智能SIM卡其实是一个小小的集成电路芯片,而每张小芯片上,除有机主知道和使用的手机号码外,还有一个由GSM手机运营商国际联盟(GSM MOU Association,简称MOU)统一掌握、每一机主自己都不知道的用以存储标志用户特征的密码(特征号码)注册参数和与鉴权、加密有关的用户的全部信息——以供手机运营商识别用户的真实身份;同时便于用户对自己的SIM卡进行加锁和解锁。<sup>②</sup>可见,惟有全球MOU组织才是该项商业秘密(即SIM卡上的内容密码及其信息)的合法权利所有人,GSM手机运营商则为该商业秘密的合法使用人。而按照MOU组织的SIM卡使用规则,在中国大陆,一码(指SIM卡所确认的电信码号)仅能制作、承载于一卡(指一张SIM卡)并同时使用于一机;不得一码制作、承载多卡并同时使用于多机。<sup>③</sup>有鉴于此,全球MOU组织对其SIM卡的加密技术和方式,即使对GSM手机运营商也是严格保密的,即移动通信运营商自己也无权针对同一手机复制出第二张SIM卡来。由此可见,非法生产该类SIM卡“解码器”者,若要令任何购买其“解码器”者破解该卡的内置密码及其信息,就须盗得MOU组织的加密、解密技术和程序。可以想见,其具体操作手段无非是采用恶意破解的黑客手法,或者采取“利诱”有关

知密人的手法窃得该项秘密。无论哪种方法,均属《中华人民共和国反不正当竞争法》第十条和《中华人民共和国刑法》第二百一十九条明令禁止的侵犯商业秘密的行为。其中,给商业秘密权利人(包括该秘密的所有人和合法使用人)“造成重大损失的”,涉嫌构成刑法第二百一十九条法定的侵犯商业秘密罪。由此可见,“特工007”在其网上广告中神侃的所谓“全球创新GSM手机号码COPY技术”,实乃“非法盗取GSM手机密码的黑术”。

“特工007”的第二环节活动是:虚假广告宣传。经过上述分析可见,至少从客观效果上看,“特工007”所销售的“三件套”,实质是在提供令人从事违法犯罪活动的工具。实践中,对此“三件套”的使用法,无外乎三类。

第一类使用法是使用该“三件套”从事“一码多卡、多机同时使用”的非法解码和复制活动;而后将其非法复制的SIM卡转售他人,从中非法牟利。这当中,被复制的原SIM卡既可能是以合法途径购得的公款报销话费的SIM卡;也可能是趁人不备,偷偷取出他人手机中的SIM卡解码并非法用作被复制卡的——而此类人等,无论其原卡是合法所得还是盗用的,其解码与复制行为都是恶意的。因为《中华人民共和国电信条例》第五十九条明文规定,任何人不得复制他人电信码号。《中华人民共和国刑法》第二百六十五条也规定,“以牟利为目的,盗接他人通信线路、复制他人电信码号的”,按刑法第二百六十四条所规定的盗窃罪定性处罚。基于此,如其解码并复制的是自己合法购得的电信码号,其行为性质应属侵犯商业秘密(相对其非法解码行为而言);情节严重者,构成侵犯商业秘密罪。如其

解码并复制的是他人的电信码号,其行为性质则具有双重性:既有侵犯商业秘密的行为;又有“以牟利为目的,复制他人电信码号的”盗窃行为。鉴于两行为之间具有手段行为与目的的行为的牵连关系,按牵连犯的“从一重处断”原则,应按盗窃罪定性处罚。情节显著轻微,不构成犯罪者,可根据《中华人民共和国治安管理处罚条例》第二十三条的规定,对其小额盗窃行为给予治安管理处罚,被复制人还可根据《民法通则》的有关规定,要求其承担侵权损害赔偿责任。

第二类使用法,是复制自己享有使用权的公款报销话费手机中的SIM卡。据报载,购买该三件套者,多作此用。这样,如其将该非法复制卡供其亲友使用,通话费用从公款中报销,则该复制人涉嫌与其亲友一起构成共同贪污(在亲友知情情况下)行为。如其所盗打的通话费用数额较大,达到贪污罪起刑点,则复制人与其盗打电话的亲友可构成共同贪污罪。其中,有身份者为主犯;无身份者为从犯。

第三类使用人为“应当知道”事实真相的恶意使用人。虽然他们可能确实不明事情真相也不懂法,买此“三件套”仅是以为自己有权解码、也有权复制自己合法购得的SIM卡。特别是,“特工007”为了欺骗潜在的买主,也为了规避法律,特地在该交易网页上声称:“此产品只限于正当用途之使用,切勿任意备份他人之SIM card手机号或协助他人非法备份SIM card手机号。若因此产品而导致任何法律之问题,消费者需自行承担,厂商概不负任何法律责任。”这一大段冠冕堂皇的话确实能蒙骗个别糊涂的使用者,因为他们购买此解码器、复制软件和可复制卡,仅仅是以为只要自己

<sup>②</sup>可参见 <http://www.135-139.com/hun11/jszi/msys.hun>

<sup>③</sup>虽然一码只能制作一卡并不得同时使用于多机,但该一张SIM卡却可不同时地用于多机。例如今天将此SIM卡置于爱立信手机使用;明天置于三星手机使用;后天置于西门子手机使用,都是合法而可行的。

出通话费用,就可以一码多卡、多机同时使用了。认为这样自己就可与家人共享一张SIM卡了。然而,事实上,其每一解码、复制过程,都是侵犯商业秘密权利所有人与使用人法定权利的过程,也是侵犯电信运营商所出售的SIM卡的使用权利的过程。因而不管其主观动机怎样——即尽管其不是出于违法犯罪动机而解码并复制出多卡,其行为不具有刑事违法性,但仍具有民事违法性。特别是“007”的网上市场与网上经营活动本属非法,此类购买人因而应当知道其所购产品为违禁品——“应当知道”因为疏忽大意或者认识能力偏低等原因而“不知道”者,仍属有民事过错的恶意使用人,行为因而仍属民事违法。

由此可见,无论将此“三件套”提供给何人,总体看,“特工007”都在事实上出售了违禁品。而《中华人民共和国广告法》第四条、第五条、第三十一条分别规定,广告主不得发布虚假的、误导他人的广告宣传;不得从事法律、法规禁止生产或销售的广告宣传活动。从事此类虚假广告宣传活动“情节严重的”,构成刑法第二百二十二条所规定的虚假广告罪。

“特工007”的第三环节活动是:非法经营。如上所述,“特工007”所出售的“三件套”,实质是有偿提供违法犯罪工具。因而,其“销售”行为应属刑法第二百五条第(四)款所规定的“其他严重扰乱市场秩序”的非法经营行为,“情节严重的”构成非法经营罪。

“特工007”的第四活动环节是:传授犯罪方法。“007”及其团伙,是以产品的“使用说明”来传授犯罪方法的。如上所述,在其出售的复制软件中,“特工007”通过其软件首先教给买受人怎样在其解码器上“破解密码”——这一“指示”过程,

就是传授特定的犯罪方法(如何侵犯商业秘密)的过程;接下来,该软件还会“指示”买受人怎样“复制SIM卡”——显然,这一“指示”,也在事实上传授着怎样复制他人电话号码这一特定的犯罪方法。

最后,“特工007”的第五活动环节是:教唆犯罪。如前所述,当记者循网站所提供的电话号码与卖主取得联系后,该卖主在电话中称:“买这种卡的主要就是一些有公款报销待遇的人,复制了之后可以将复制卡赠送给自己的亲友,话费由单位报销。此外,就是用来盗打他人电话。买这种复制器做卡,用来盗打他人电话的很多,基本上都是为了省钱”。这一段话,不但印证了其网上销售广告上所谓“此产品只限于正当用途,切勿任意备份他人之SIM card手机号”的虚伪性和欺骗性,还是赤裸裸的犯罪教唆。换言之,每一恶意购买者,实则在事实上与该售卖人达成了共同侵犯商业秘密或共同盗窃的心照不宣的违法犯罪合意。销者因而涉嫌构成共同犯罪的教唆犯和帮助犯(提供犯罪工具);买者如将其所购买的产品付诸解码和复制行为,也涉嫌构成共犯中的实行犯。

当然,上述各活动环节,在实践中可能发生相互交错或竞合的情况,不排除其中某些环节因情节显著轻微不构成犯罪(仅属民事或经济违法);也不排除某些环节因情节轻微、应与其他重度犯罪行为所吸收。但此一具有共犯性质的连环违法犯罪活动,确也涉嫌触犯多个或共同或单独的刑法罪名。

### 三、由本案所引发的法律思考

疾速发展的网络世界充满了二重性:它既是无奇不有、无所不在、包罗万象的;又是虚拟的、数字的、无边无涯的。人们在网上的行为,因

而既是公开的、又是隐秘的;既是永恒的、又是稍纵即逝的。于是,从一般法理视界看,当今社会中,既针对现实、又针对网络世界的法律,因网络世界的虚拟性、隐秘性、稍纵即逝性而很难操作于网络世界。惟其如此,网络世界正在以其独特的运作方式向每一位法学工作者发出崭新的研究课题,那就是:认真审视和梳理哪些法律法规难于甚而不能有效适用于计算机Byte世界,进而考量有无必要、并怎样通过专门的网络立法来补救之。例如美国于1998年5月14日通过了《网络免税法案》,规定3年内禁止联邦和州政府对Internet访问征收新税,Byte税以及对电子商务征收的重复或附加税。<sup>④</sup>从一定意义看,它弥合了网上征税困难与疾速发展电子商务的法律裂痕,进而,它一方面调和了立法与守法的二致;同时免去了法律因而丧失其基本威权的弊端。然而,并不是所有立法与守法的矛盾都宜于通过法律的转向来消极调和的。恰恰相反,就一般意义看,根据实情需要,出台更多的、专门的网络法律规范,以积极调适规范与有关禁止性行为的冲突,势在必行。

总而言之,本案引人深思的第一层次问题是:全面强化网络广告的规范与管理,应当提上议事日程。眼下,专门的网络广告管理法规,已经见之于某些地方行政法规之中。例如,北京、浙江均出台了有关网络广告管理办法。然而,问题在于:

其一,诸如此类的网络广告管理法规的空间效力范围太过狭窄——仅限于国内个别行政区域,而网络世界是无垠的,从而此类网络规范难以产生实效。例如浙江、北京市的网民任何时候均可登录任何地方的任何网络;而囿于浙江、北京等网络广告法规的限制,该地的经营性网络广告提供商也可以到外地

<sup>④</sup>2001年10月,美国国会再次通过延长该法案的有效实行期限两年,即其有效期将延至2003年11月1日。

注册网络经营业务,在外地设计、制作、发布网络广告同样可影响于全国甚而整个网络世界。由此可见,网络的特殊性,决定了网络法律规范“一体化”的重要性。要有效杜绝网络上的虚假广告等违法犯罪行为,还有待全国性的网络广告管理法规的统一颁行。

其二,即便是现行的地方性《网络广告管理暂行办法》,也有待在实践中改革完善。例如北京市的《办法》第九条虽然规定互联网信息服务提供者“不得在网站上发表法律、行政法规禁止发布广告的商品或者服务”,但法律、行政法规禁止发布广告的商品或者服务是什么呢?是否包括本案“007”所销售的用于伪造SIM卡的犯罪工具呢?显然,就此笼统的规定,不得而知。有鉴于此,今后无论是地方性还是全国性的网络广告管理法规,都宜于针对“数字商品”的高科技性、隐秘性,制定出更加便于操作的禁止发布的范围和界定原则来。进而,此类网络广告管理法规才能同《中华人民共和国广告法》第四条、第五条、第三十一条衔接起来,再同刑法第二百二十二条衔接起来,刑法也才能真正成为广告法及其配套规范的保障法。

其三,网络内外的广告管理机构——各级工商行政管理机关的广告监督部门,宜组织专人对各类难于识别真相的高科技“产品”——特别是各类“复制品”广告进行定期定向监测,必要时可以“消费者”身份摸底调查,以便一旦发现违法广告,即可下载取证,同时遏止其连锁违法犯罪活动。

本案发人深思的第二层次问题是:刑事立法上可考虑增设“网上提供犯罪工具罪”。基本理由是:对有

偿提供犯罪工具的行为,尚可适用现行刑法第二百二十五条,按非法经营罪定性处理。而对网上无偿“提供犯罪工具者”,法律该怎样面对呢?例如稍微懂行一些的人会发现,网络上往往充斥着各类打通或穿透整个计算机系统的工具,而该犯罪工具的“受众”是不特定的、虚拟的。<sup>⑤</sup>因而,对此类“提供”行为,司法上不可能按照传统的共同犯罪的“帮助犯”来处理,但通过现代网络监测系统,我们并非不能侦破此类恶意提供者。随着互联网的普及和社会各行各业对计算机信息系统依赖程度的日益提高,此类今天看来还是“准犯罪”的行为,明天可能酿发大规模的社会危害,因而有必要未雨绸缪。

本案尚待思考的最后议题是:现行刑法是否有必要填补“伪造SIM卡活动”的空白。通过以上连环违法犯罪活动的解剖,细心者可能已经发现,倘若“三件套”的买受人,明知故犯地将此“三件套”用于“复制”自己合法购得的SIM卡,则无论其“复制”多少张,哪怕是“1码16卡”,只要他没有用其去卖钱“牟利”,其行为就只构成民事侵权,即其仅仅侵犯了商业秘密权利人的合法权益,包括权利所有人与权利使用人的权益。权利人——例如移动通信运营商如感到自己的合法权益受到损害,有权提起损害赔偿诉讼。但是,鉴于该买受人没有从事经营性活动,他就不是“经营者”,因而他不能成为《反不正当竞争法》调控与打击的对象。再者,由于其复制的并非“他人”码号而是自己的码号,因而也不能成立因非法复制他人码号而转化的“盗窃”行为。然而,此类行为在性质上与其说是“复制”,毋宁称其为“伪造SIM卡的行为”,据此,

刑法是否宜于作出犯罪设计呢?例如在刑法中增设“伪造SIM卡罪”?

笔者认为,根据刑法的谦抑性原则,能以民事、经济法律规范调控的行为就不付诸刑法。英国哲学家边沁有一句名言“温和的法律能使一个民族的生活方式具有人性;政府的精神会在公民中间得到尊重。”这句话可以说是对刑法谦抑性价值的最好脚注。有鉴于此,对上述没有从事“非法牟利”活动的少量的“伪造SIM卡行为”,鉴于其危害情节显著轻微,不宜设定为刑事犯罪。

但是,应当强调的是,假若复制人所复制的不是一般的GSM手机SIM卡而是“包月卡”,<sup>⑥</sup>情况则不然。因为此种场合,复制人虽然复制的是自己的SIM卡,但用其伪造的包月SIM卡所打电话费用却不再由码号人自己承担,而是移动通信运营商承担。移动通信运营商原本仅承诺一码一卡的包干使用,未曾承诺也未曾料及买卡人会以“一码伪造出多卡”来无限使用。因而,此类行为实质是盗用电信运营商的码号、用公款打电话。<sup>⑦</sup>据此,对此类行为,如其盗打数额达到盗窃罪起刑点时,应根据刑法第二百六十五条定性为(转化)盗窃罪。而被盗打的移动通信运营商,则可通过有关程序索回自己因被盗打而损失的移动通信费用。

#### [参考文献]

[1] (英) 吉米·边沁. 立法理论——刑法典原理[M]. 北京: 中国人民大学出版社, 1993. 150.

[责任编辑:李和仁]

⑤有关此问题的探讨,详见屈学武:《因特网上的犯罪及其遏制》,《法学研究》2000年第4期。

⑥包月卡,指由移动通信运营商发行的、每月每卡缴纳定额话费后,该卡则可置于某一GSM手机上作一定程度、一定范围内的无上限通话使用。例如某些城市实行的每卡每月缴纳300元后,该SIM卡则可按月包(市话)接听或按月包发话,等等。

⑦鉴于迄今为止,在中国享有移动通信经营权者,均为国家公用数字通信网的电信运营商,如中国联通公司、中国移动通信公司等,因而这里因盗窃流失的资财,实为国家财产。