- 责任编辑 金勇 E-mail:fzbwjh@126.com



欧盟:明确界定网络犯罪行为

欧盟制定了多项法律,对网络犯罪行为进行明确界定。2001年11月,由26个欧盟成员国以及美国、加拿大、日本和南非共30个国家在布达佩斯缔结《网络犯罪公约》。其中规定,缔约国应对以下九类网络犯罪行为给予刑事处罚:

非法进入。当针对整个计算机系统或 其任何部分的访问是未经授权而故意进行 时,认定为犯罪行为。

非法截取。此类行为包括非法截取电 脑传送的"非公开性质"电脑资料。

资料干扰。包含任何故意毁损、册 、破坏、修改或隐藏电脑资料的行为。

系统干扰。利用电脑系统传送电脑病毒、蠕虫、特洛伊木马程序或滥发垃圾电子邮件,构成"系统干扰"的行为。

设备滥用。包含生产、销售、发行或以 任何方式提供任何从事上述各项网络犯罪设 备的行为。

伪造电脑资料。包括任何虚伪资料输 人、更改、删改、隐藏电脑资料,导致相关 资料丧失正确性的行为。

电脑诈骗。包括任何有诈骗意图的资料 输入、更改、删除或隐藏任何电脑资料,或 干扰电脑系统的正常运作,为个人谋取不法 利益而导致他人财产损失的行为。

儿童色情犯罪。包括一切在电脑系统生 产、提供、发行或传送、取得及持有儿童色 情资料的行为。

侵犯著作权及相关权利行为。此项规定 包括数条保障智慧财产权、国际公约列为侵 犯著作权的行为。



韩国:从源头上遏制网络诈骗

近年来,韩国陆续推出了一系列法律 制度,以便从源头上遏制电信网络诈骗犯 罪。

韩国从 2001 年起,采取一户一网、机号一体的手机号码人网登记制,要求广告商在发送短信时,必须注明"广告"字样,如果手机用户不愿意接收该信息,所产生的电话费由广告商承担。同时规定,在每晚9时至第二天上午8时之间,广告商不得发送短信广告。对滥发垃圾短信者,可处以最高8500美元的罚款。

韩国从 2002 年通过立法推行网络实名制,要求网络用户必须通过实名认证才能在网上发布信息。实名制规范了网民行为, 净化了网络环境,在预防和查处网络犯罪 方面取得了良好效果。

推行"延迟提款"制度。所谓"延迟提款",就是大额提款将被冻结 30 分钟。金融监管部门为应对电信网络诈骗频发的形势,还多次进行政策调整,现在已将"延迟提款"的金额限度定为 100 万韩元,即在收到 100 万韩元以上银行转账指令后,若想将钱从自动提款机里取出来,需要等待 30 分钟以上。

韩国刑法中关于电信诈骗的规定很有针对性。如利用电脑输入虚假信息或否定的命令或没有权限地输入信息,变更信息处理,从而获得财产上的利益或让第三者获得利益的,处十年以下的徒刑或 2000 万韩元以下罚款。

澳大利亚:运用科技手段侦破案件

澳大利亚采取多种手段全方位预防诈骗案件的发生,并运用科技手段侦破案件。

拒绝来电制度。澳大利亚政府研发出具有 电话保护功能的软件,用户可根据自身的需 要,自主选择屏蔽或拒接业务推销、保险及其 他涉嫌诈骗的电话。

澳大利亚竞争和消费委员会建立了专门防 控电信诈骗的机构。若在境内遭受侵害,受害 人可以直接登录该机构的官网进行登记报案, 报案信息可以同时被90个执法部门所掌握。

另外,各州警察部门设置了专门针对电信诈骗案件的调查、处理机构。数据深挖技术是一项通过检索庞大的数据库查找异常信息,并进行深度整理和分析的技术,运用该技术可以侦破电信诈骗案件。特征勾画技术可以通过作案者的行为特征来分析其目的,例如,通过分析电话诈骗分子的声音大小、语速快慢、紧张程度,来确定是初犯还是惯犯。

日本:电信服务提供商须承担赔偿责任

日本根据电信网络诈骗犯罪分子的犯罪方 式,制定了多项法律进行处罚。

日本刑法使用电子计算机诈骗罪规定,用 电子计算机输入虚假信息或者不正当指令,从 而制作出有关财产权得失或变更的不真实的电 信记录,或者提供有关财产权得失或变更的虚 假电信记录以供他人处理事务,因而获取财产 性不法利益或使他人获取的,处十年以下徒 刑。未遂同罚。

日本专门研发了一种诈骗电话识别软件, 其特点是搜集手机高频率诈骗用语,建立庞大 的数据库,形成自动对比识别功能。该软件能通过来电者语调的变化,判断是否为诈骗电话,如果识别出该电话是诈骗电话,就会自动报警

日本《关于特定电信服务提供商之损害赔偿责任限制与信息发送者资料披露法》规定,电信服务提供商必须承担赔偿责任。受害者也有权向电信服务供应商请求停止该类信息的输出。2007年,日本通过《假冒账户存入受害者救济法》,授权银行对可疑账户进行冻结,并对受害人的受骗金额返回等作出规定。

德国:健全防骗法律体系

德国针对电信网络诈骗犯罪颁布和修订 了多项法律,形成了完备的法律体系,同时 还落实了多项管控措施。

在德国,国家、地州层面都有相应的立法,如《防止个人资料处理滥用法》《州数据保护法》《皖邦数据保护法》等。《德国刑法典》设定了6种网络犯罪罪名,分别为刺探数据罪、截留数据罪、预备刺探或截留数据罪、计算机诈骗罪、数据篡改罪和破坏计算机罪。法定刑为五年以下自由刑或者罚

金刑。当情形特别严重时, 法定刑为六个月以 上十年以下自由刑。

德国联邦信息技术安全局为了防止公民的 个人资料被不法分子盗取、利用,专门设置了 服务市民的网络平台,以提高公民的防范能力。

德国各地的消费者保护部门十分重视对电信诈骗的监管,建立了相关信息库。实行实名登记制度,用户在银行开户,或订立手机、网络等服务合同时,要签订"信用合同"。如果个人信用评分太低,用户就无法开户。

新加坡:严格规范网上行为

新加坡颁布了一系列法律规范网上行为, 遏制电信网络犯罪。

新加坡颁布了《网络行为法》和《互联网操作规则》。《网络行为法》规定了网民上网应遵守的义务和网络服务商的行业准则。《互联网操作规则》规定,网络运营商对网络传播的内容负有审查、报告和协助司法机关执法的义务。

如发现有涉及违法犯罪的网络信息,必须 及时向司法机关报告,并且需要配合执法部门 屏蔽和删除这些信息。同时,还明确规定网站 禁止发布的内容,如禁止发布危害国家安全、 涉及恐怖暴力的内容等。

2012 年 10 月,新加坡出台《个人信息保护法案》。该法案明确规定相关机构在使用或披露个人资料时必须得到当事人的同意。

新加坡警方和商业事务局联合成立反诈骗中心,该中心可迅速冻结涉及诈骗的银行户头,切断诈骗者使用的电话线。要求电信公司和电子商务公司依法主动配合执法。电信公司在警方提出要求的当日内,必须切断可疑电话线;电子商务平台必须主动监测和删除虚假账号,从源头制止诈骗案件的发生。

来源:人民法院报