

# ĐẶC ĐIỂM NHẬN DẠNG TỘI XÂM NHẬP TRÁI PHÉP VÀO MẠNG MÁY TÍNH, MẠNG VIỄN THÔNG HOẶC PHƯƠNG TIỆN ĐIỆN TỬ CỦA NGƯỜI KHÁC Ở VIỆT NAM HIỆN NAY

HỒ TRỌNG HỮU  
Khoa Luật, Trường Đại học Vinh

Nhận bài ngày 02/7/2021. Sửa chữa xong 06/7/2021. Duyệt đăng 11/7/2021.

## Abstract

*In recent times, crimes in the field of information technology, telecommunication network in general and crimes in illegal infiltration into the computer network, telecommunication network, or electronic device of another person tends to have an increase and be more complicated with many new methods and manners. In this paper, an author analyzes the identification features of illegal infiltration into the computer network, telecommunication network, or electronic device of another person in Vietnam today. This is the basis for users and state management agencies having measures to ensure safety in the field of information technology and telecommunication networks.*

**Keywords:** *The Criminal Code, legal signs, cybercrime, Article 289 the Criminal Code.*

## 1. Khái niệm tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác

Hiện nay, có nhiều quan điểm khác nhau về tội phạm trong lĩnh vực công nghệ thông tin (CNTT), mạng viễn thông. Theo Từ điển luật học của Viện khoa học pháp lý, Bộ Tư pháp, tội phạm vi tính là “tội phạm xâm phạm trật tự an toàn xã hội được thực hiện trong lĩnh vực công nghệ thông tin, có hành vi khách quan liên quan đến sử dụng máy tính và các tính năng của nó gây rối loạn hoạt động, phong tỏa hoặc làm biến dạng, hủy hoại các dữ liệu hoặc đưa vào mạng những thông tin trái với quy định của pháp luật gây hậu quả nghiêm trọng”[6]. Tại khoản 1, Điều 8, Bộ luật Hình sự năm 2015 sửa đổi, bổ sung năm 2017, quy định [2]: “Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự, do người có năng lực trách nhiệm hình sự sử dụng công nghệ thông tin, mạng viễn thông thực hiện với lỗi cố ý, xâm phạm an toàn mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử”.

Theo khoản 1 Điều 289 Bộ luật Hình sự năm 2015, tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác là “hành vi cố ý vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác do người có năng lực trách nhiệm hình sự thực hiện nhằm chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của phương tiện điện tử; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ”.

## 2. Quá trình hình thành các quy định về tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác trong pháp luật hình sự Việt Nam

Trong quá trình xây dựng và hoàn thiện văn bản quy phạm pháp luật, hoạt động truy cập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử chưa được quy định trong Bộ luật Hình sự năm 1985 và Bộ luật Hình sự năm 1999.

Tội phạm trong lĩnh vực CNTT, mạng viễn thông được quy định lần đầu tiên trong Bộ luật Hình sự năm 1999 gồm 3 điều khoản về các tội: Điều 224 - Tội tạo ra và lan truyền, phát tán các chương trình

vi - rút tin học); Điều 225 - Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử; Điều 226 - Tội sử dụng trái phép thông tin trên mạng và trong máy tính) [1].

Bộ luật Hình sự năm 1999 sửa đổi, bổ sung năm 2009 đã bổ sung thêm 2 quy phạm pháp luật mới về tội phạm trong lĩnh vực CNTT, mạng viễn thông, bao gồm: Điều 226a - Tội truy cập bất hợp pháp vào mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số của người khác và Điều 226b - Tội sử dụng mạng máy tính, mạng viễn thông, mạng Internet hoặc thiết bị số thực hiện hành vi chiếm đoạt tài sản. Bộ luật Hình sự năm 2009 cũng sửa đổi Điều 224, Điều 225 và Điều 226 theo hướng thiết kế điều luật cụ thể hơn, rõ ràng hơn, đưa thêm vào cấu thành tăng nặng một số tình tiết định khung. Như vậy, đến lần sửa đổi bổ sung của Bộ luật Hình sự năm 2009, hành vi truy cập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử mới chính thức được ghi nhận trong hệ thống pháp luật nước ta.

Tại Bộ luật Hình sự năm 2015, sửa đổi bổ sung năm 2017, tội phạm trong lĩnh vực CNTT, mạng viễn thông được quy định tại Mục 2, Chương XXI từ Điều 285 đến Điều 294 gồm các tội danh sau: *Điều 285* - Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật; *Điều 286* - Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; *Điều 287* - Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; *Điều 288* - Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông; *Điều 289* - Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác; *Điều 290* - Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản; *Điều 291* - Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng; *Điều 292* - Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông; *Điều 293* - Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh; *Điều 294* - Tội cố ý gây nhiễu có hại. Như vậy: tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác được quy định tại Điều 289 Bộ luật Hình sự hiện hành [2].

### **3. Cấu thành tội phạm của tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác**

Làm rõ cấu thành tội phạm của tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác có ý nghĩa quyết định trong việc phân biệt tội phạm và là căn cứ pháp lý để tòa án kết án một người có phạm tội hay không. Khoa học về pháp luật hình sự xác định có bốn yếu tố cấu thành tội phạm, đó là: chủ thể tội phạm, mặt khách quan của tội phạm, mặt chủ quan của tội phạm và khách thể của tội phạm. Bốn yếu tố cấu thành tội phạm có mối liên hệ mật thiết, bổ trợ cho nhau.

#### **3.1. Khách thể của tội phạm**

Những hành vi quy định thuộc mặt khách quan xâm phạm đến chế độ quản lý an ninh mạng của người sử dụng, và quan hệ xã hội này được pháp luật hình sự bảo vệ.

#### **3.2. Mặt khách quan của tội phạm**

Hành vi khách quan của tội phạm là hành vi truy cập vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử mà không được sự đồng ý của người chủ sở hữu hoặc người quản lý điều hành mạng máy tính, mạng viễn thông hoặc phương tiện điện tử đó. Hành vi này được thực hiện thông qua các thủ đoạn như: (i) Vượt qua cảnh báo là vượt qua thông báo không cho phép người không có thẩm quyền truy cập vào cơ sở dữ liệu; (ii) Vượt qua mã truy cập là vượt qua những điều kiện bắt buộc đáp ứng một tiêu chí chuẩn nhất định trước khi sử dụng, truy cập tới thiết bị, nội dung dữ liệu được bảo vệ; (iii) Vượt qua tường lửa để xâm nhập trái phép, trong đó, tường lửa là tập hợp các thành phần hoặc một hệ thống các trang thiết bị, phần mềm hoặc phần cứng được đặt giữa hai hay nhiều mạng nhằm kiểm soát tất cả những kết nối từ bên trong ra bên ngoài và ngược lại, đồng thời ngăn

chặn việc xâm nhập, kết nối trái phép; (iv) Sử dụng quyền quản trị của người khác là sử dụng quyền quản lý, vận hành, khai thác và duy trì hoạt động ổn định hệ thống mạng máy tính, mạng viễn thông của cá nhân, tổ chức; (v) Các phương thức xâm nhập trái phép khác như bẻ khóa, trộm mật khẩu, mật mã của người khác để xâm nhập trái phép hoặc xâm nhập vật lý như mở khóa cửa vào phòng, khu vực không thuộc phạm vi để truy cập vào mạng máy tính, mạng viễn thông, phương tiện điện tử.

Sau khi xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác, người phạm tội có thể thực hiện một trong những hoạt động:

- Chiếm quyền điều khiển mạng máy tính, mạng viễn thông hoặc phương tiện điện tử. Sau khi xâm nhập vào mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội sẽ chiếm quyền điều khiển của mạng máy tính, mạng viễn thông hoặc phương tiện điện tử đó.

- Can thiệp vào chức năng hoạt động của phương tiện điện tử. Can thiệp vào chức năng hoạt động của phương tiện điện tử là những hành vi làm cho phương tiện điện tử không thể hoạt động bình thường. Để xử lý thông tin, các phương tiện điện tử thường có bốn chức năng hoạt động cơ bản: nhận thông tin, xử lý thông tin, xuất thông tin, lưu trữ thông tin. Người phạm tội có thể can thiệp vào bất cứ chức năng nào làm cho phương tiện điện tử đó hoạt động sai như can thiệp vào chức năng nhập thông tin bằng cách nhập vào thông tin sai lệnh để cho ra kết quả xử lý thông tin không đúng, như tăng thêm số ngày làm việc để được trả lương cao hơn; can thiệp để quá trình xử lý thông tin bị sai dẫn đến kết quả sai.

- Lấy cắp dữ liệu điện tử. Sau khi xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử của nạn nhân, người phạm tội trộm cắp dữ liệu điện tử của mạng máy tính, mạng viễn thông, phương tiện điện tử đó. Trộm cắp dữ liệu được thực hiện bằng mọi thủ đoạn làm mất tính bí mật của dữ liệu điện tử như đọc trộm dữ liệu, nghe lén, sao chép trộm dữ liệu...

- Thay đổi, huỷ hoại dữ liệu điện tử. Dữ liệu điện tử chỉ có giá trị khi có đầy đủ tính bí mật, tính toàn vẹn và tính sẵn sàng. Khi bị thay đổi hoặc huỷ hoại, dữ liệu điện tử sẽ mất đi tính toàn vẹn và không còn giá trị. Trường hợp này, sau khi xâm nhập trái phép mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội đã thay đổi, huỷ hoại làm mất đi tính toàn vẹn của dữ liệu điện tử của mạng máy tính, mạng viễn thông, phương tiện điện tử đó.

- Làm giả dữ liệu điện tử. Sau khi xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử, người phạm tội đã chuyển vào đó các dữ liệu điện tử giả. Đây là hình thức tấn công nhằm vào tính xác thực của dữ liệu điện tử. Tính xác thực của thông tin, dữ liệu điện tử thể hiện ở chỗ thông tin, dữ liệu được gửi đi trong mạng máy tính hoặc mạng viễn thông phải do chính người gửi tạo ra. Nếu thông tin, dữ liệu do người khác tạo ra và gửi đi trong mạng máy tính, mạng viễn thông sẽ tạo ra sự nhầm lẫn cho người nhận như nhận được cảnh báo sai lũ lụt, động đất, dịch bệnh,... dẫn đến hoảng loạn, sơ tán dân chúng.

- Sử dụng trái phép các dịch vụ. Người phạm tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông, phương tiện điện tử đang cung cấp các dịch vụ sử dụng có thu tiền để sử dụng trái phép các dịch vụ đó mà không phải trả tiền như: dịch vụ viễn thông, xem phim, nghe nhạc, mua vé, đặt hàng,...

Ngoài hành vi phạm tội cần lưu ý đến công cụ, phương tiện phạm tội: các đối tượng sử dụng mạng máy tính, mạng viễn thông làm công cụ, phương tiện để thực hiện hành vi phạm tội.

### **3.3. Mặt chủ quan của tội phạm**

Theo quy định của Bộ luật Hình sự năm 2015, tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác cũng như các loại tội phạm khác thuộc nhóm tội này luôn là lỗi cố ý, không có hình thức lỗi vô ý. Tội phạm có thể được thực hiện với lỗi cố ý trực tiếp hoặc cố ý gián tiếp. Khi thực hiện hành vi phạm tội, người phạm tội nhận thức được hành vi của mình là nguy hiểm cho xã hội, nhận thức được hậu quả nguy hiểm cho xã hội có thể xảy ra (đối với những tội có cấu thành vật chất) nhưng vẫn thực hiện hành vi phạm tội đó và mong muốn hoặc có ý thức bỏ mặc cho hậu quả xảy ra. Trường hợp, hành vi được thực hiện với lỗi vô ý sẽ không bị coi là tội phạm.



Nội hàm cụm từ “cố ý” được quy định trong nội dung điều luật đã thể hiện rõ người thực hiện hành vi phạm tội rõ hành vi xâm nhập trái phép của mình vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác là nguy hiểm cho xã hội, thấy trước hậu quả của hành vi đó là làm cho mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác bị xâm nhập trái phép, chiếm quyền sở hữu và mong muốn hậu quả đó xảy ra.

Bên cạnh đó, khi xem xét “tội danh” thì động cơ và mục đích của tội phạm không phải là dấu hiệu bắt buộc.

### **3.4. Chủ thể của tội phạm**

Người phạm tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác hoàn toàn phải là cá nhân không thuộc tình trạng mất năng lực trách nhiệm hình sự được quy định tại Điều 21 Bộ luật Hình sự năm 2015, tức là người đó phải trong độ tuổi quy định và thực hiện hành vi nguy hiểm cho xã hội trong khi đủ khả năng nhận thức và điều khiển hành vi của mình. Về độ tuổi được quy định như sau:

- Đối với người từ đủ 14 tuổi đến dưới 16 tuổi phải chịu trách nhiệm hình sự đối với tội rất nghiêm trọng và đặc biệt nghiêm trọng quy định tại Điều 289 Bộ luật Hình sự năm 2015

- Đối với người từ đủ 16 tuổi trở lên, có năng lực trách nhiệm hình sự phải chịu trách nhiệm hình sự đối với trường hợp phạm tội thuộc khoản 3 Điều 289 Bộ luật Hình sự năm 2015

## **4. Đặc điểm của tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác**

### **4.1. Tội phạm được thực hiện mà không bị giới hạn về không gian và thời gian**

Môi trường không gian mạng được kết nối toàn cầu thông qua mạng internet, mạng viễn thông quốc tế. Do đó, người phạm tội có thể ở một chỗ nhưng lại thực hiện tội phạm ở những địa điểm khác nhau, có khi ở các nước khác nhau. Với tốc độ kết nối internet và viễn thông như hiện nay, trong một thời gian ngắn, người phạm tội có thể thực hiện tội phạm và gây ra thiệt hại cho nhiều nạn nhân khác nhau trong phạm vi toàn thế giới. Như vậy, tội phạm có thể được thực hiện ở bất kỳ thời gian nào và không bị giới hạn bởi phạm vi không gian.

### **4.2. Khách thể của tội phạm là quan hệ xã hội đảm bảo an toàn của mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử bị xâm phạm**

Trường hợp người phạm tội sử dụng CNTT, mạng viễn thông để thực hiện tội phạm xâm phạm an ninh quốc gia, danh dự, nhân phẩm của con người, trật tự quản lý kinh tế, trật tự công cộng thì không coi là tội phạm trong lĩnh vực CNTT, mạng viễn thông, mà thuộc cấu thành tội phạm của nhóm nhóm tội phạm tương ứng.

Đối tượng tác động của tội phạm trong lĩnh vực CNTT, mạng viễn thông nói chung bao gồm các nhóm sau: dữ liệu điện tử, mạng máy tính, mạng viễn thông, phương tiện điện tử.

### **4.3. Hành vi khách quan của tội phạm rất đa dạng bằng mắt thường không thể nhìn thấy mà phải thông qua phương tiện, thiết bị kỹ thuật**

Với sự phát triển của khoa học kỹ thuật trong đó có lĩnh vực CNTT và mạng viễn thông, các đối tượng có nhiều cơ hội để thực hiện hành vi phạm tội. Trong môi trường không gian mạng, con người chỉ có thể thực hiện các hành vi của mình thông qua các công cụ, biện pháp kỹ thuật là mạng máy tính, mạng viễn thông, phương tiện điện tử, dữ liệu điện tử. Do đó để thực hiện tội phạm này, người phạm tội buộc phải sử dụng CNTT, mạng viễn thông làm công cụ, phương tiện phạm tội. Đây cũng là dấu hiệu để phân biệt giữa tội phạm trong lĩnh vực CNTT, mạng viễn thông với các tội phạm truyền thống khác.

### **4.4. Hậu quả của tội phạm được thể hiện thông qua sự biến đổi tình trạng bình thường của đối tượng tác động của tội phạm thường rất nặng nề và khó bị phát hiện**

Hậu quả nguy hiểm cho xã hội của tội phạm có thể mô tả bằng định tính hoặc định lượng. Mô

tả định tính là mô tả về tính chất nguy hiểm hoặc nghiêm trọng của hậu quả đó. Mô tả định lượng là mô tả hậu quả của tội phạm bằng các con số cụ thể. Việc quy định về thiệt hại gây ra cho khách thể dẫn đến sự biến đổi tình trạng bình thường của đối tượng tác động thể hiện qua mô tả các dấu hiệu phản ánh hậu quả của tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác, gồm: hoạt động bình thường của cơ quan, tổ chức, cá nhân; an toàn thông tin, dữ liệu mạng máy tính, mạng viễn thông, phương tiện điện tử; số lượng người dùng, phương tiện điện tử bị ảnh hưởng được phản ánh thông qua số lượng thực tế gây ra; lợi ích vật chất bị hủy hoại, hư hỏng, mất mát phản ánh thông qua giá trị bằng tiền những hư hỏng, hủy hoại, mất mát do tội phạm gây ra; lợi ích bất chính mà người phạm tội thu được được định lượng bằng tiền đối với mọi lợi ích bất chính mà người phạm tội có được do phạm tội trong lĩnh vực CNTT, mạng viễn thông.

**4.5. Tội phạm được thực hiện với lỗi cố ý**

Khi thực hiện tội phạm, người phạm tội nhận thức rõ hành vi sử dụng CNTT, mạng viễn thông để phạm tội là hành vi nguy hiểm cho xã hội, các đối tượng thấy trước hậu quả của hành vi đó có thể xảy ra, đồng thời mong muốn hoặc có ý thức để mặc cho hậu quả đó xảy ra. Do vậy, tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác luôn được thực hiện với lỗi cố ý.

**4.6. Chủ thể của tội phạm là những chủ thể có kiến thức, hiểu biết nhất định về CNTT, mạng viễn thông**

Chủ thể của tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác là chủ thể thường. Tuy nhiên, trong giai đoạn đầu khi tội phạm này mới xuất hiện, không cá nhân nào đủ điều kiện để sở hữu máy tính riêng nên những người có thể sử dụng máy tính đều là những người có chuyên môn cao, được đào tạo để sử dụng máy vi tính. Người phạm tội cũng chính là số ít những người có hiểu biết này. Đến thời điểm hiện nay, CNTT và mạng viễn thông đã phổ biến và dễ sử dụng, nhưng để thực hiện các hành vi phạm tội hết sức tinh vi, che giấu để không bị phát hiện đòi hỏi đối tượng phải là người có hiểu biết về lĩnh vực CNTT, mạng viễn thông.

Đặc biệt, những người trẻ tuổi thường là chủ thể thực hiện do họ có các điều kiện để tiếp xúc với CNTT và mạng viễn thông nhiều hơn các nhóm đối tượng khác trong xã hội.

**5. Tình hình phạm tội và khung hình phạt được quy định trong pháp luật hình sự ở Việt Nam**

Tội phạm trong lĩnh vực CNTT, mạng viễn thông diễn biến ngày càng phức tạp với nhiều phương thức, thủ đoạn phạm tội mới, hoạt động có tính chất xuyên quốc gia và xảy ra trên nhiều lĩnh vực, gây thiệt hại lớn. Thiệt hại được thể hiện thông qua sự biến đổi tình trạng bình thường của đối tượng tác động của tội phạm. Theo số liệu thống kê của Tòa án nhân dân tối cao, năm 2009 đến năm 2014 có 78 vụ, với 214 bị cáo; từ năm 2015 đến năm 2020 có 367 vụ án với 719 bị cáo bị xét xử trong lĩnh vực CNTT, mạng viễn thông ở Việt Nam [3].

Theo khảo sát, khoảng 70% các nước và nhiều văn bản pháp luật quốc tế có quy định hành vi xâm nhập mạng máy tính bị coi là tội phạm, không kể có mục đích cụ thể hay không. Vì bản thân hành vi xâm nhập trái phép đó chỉ để đọc dữ liệu thôi đã làm mất đi tính bí mật của dữ liệu điện tử và điều đó cũng nguy hiểm cho xã hội và bị coi là tội phạm. Tại Việt Nam, riêng số lượng vụ án được đưa ra xét xử về tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác từ năm 2009 đến năm 2020 là 17 vụ với 34 bị cáo, cụ thể như sau:

Năm	Số vụ	Số bị cáo
2009 - 2017	10	25
2018 - 2020	7	9

*Bảng thống kê số lượng vụ án và bị cáo đã xét xử sơ thẩm*

Qua thống kê thấy rằng, trong 9 năm từ năm 2009 đến cuối năm 2017, số vụ án được xét xử về tội

xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác có tỉ lệ ít hơn so với giai đoạn 2018 – 2020. Tuy nhiên, tỉ lệ bị cáo trên vụ án thì giai đoạn 2009 – 2017 có tỉ lệ cao hơn (trung bình trên 2 bị cáo/ vụ) [3].

Ở Việt Nam tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác được chia thành ba khung, như sau: [2]

– *Khung một*: Người nào cố ý vượt qua cảnh báo, mã truy cập, tường lửa, sử dụng quyền quản trị của người khác hoặc bằng phương thức khác xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác chiếm quyền điều khiển; can thiệp vào chức năng hoạt động của phương tiện điện tử; lấy cắp, thay đổi, hủy hoại, làm giả dữ liệu hoặc sử dụng trái phép các dịch vụ, thì bị phạt tiền từ 50.000.000 đồng đến 300.000.000 đồng hoặc phạt tù từ 01 năm đến 05 năm.

– *Khung hai*: Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tiền từ 300.000.000 đồng đến 1.000.000.000 đồng hoặc bị phạt tù từ 03 năm đến 07 năm: có tổ chức; lợi dụng chức vụ, quyền hạn; thu lợi bất chính từ 200.000.000 đồng đến dưới 500.000.000 đồng; gây thiệt hại từ 300.000.000 đồng đến dưới 1.000.000.000 đồng; đối với trạm trung chuyển internet quốc gia, hệ thống cơ sở dữ liệu tên miền và hệ thống máy chủ tên miền quốc gia; tái phạm nguy hiểm.

– *Khung ba*: Phạm tội thuộc một trong các trường hợp sau đây, thì bị phạt tù từ 07 năm đến 12 năm: đối với hệ thống dữ liệu thuộc bí mật nhà nước; hệ thống thông tin phục vụ quốc phòng, an ninh; đối với cơ sở hạ tầng thông tin quốc gia; hệ thống thông tin điều hành lưới điện quốc gia; hệ thống thông tin tài chính, ngân hàng; hệ thống thông tin điều khiển giao thông; thu lợi bất chính 500.000.000 đồng trở lên; gây thiệt hại 1.000.000.000 đồng trở lên.

Ngoài việc bị xử phạt một trong các hình phạt chính nêu trên, tùy từng trường hợp cụ thể người phạm tội còn có thể bị: phạt tiền từ 5.000.000 đồng đến 50.000.000 đồng, cấm đảm nhiệm chức vụ, cấm hành nghề hoặc làm công việc nhất định từ 01 năm đến 05 năm.

Việc xem xét các đặc điểm của tội phạm trong lĩnh vực CNTT và mạng viễn thông nói chung và tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác nói riêng sẽ cung cấp bộ công cụ để nhận dạng các tội phạm cụ thể. Bên cạnh đó, việc nghiên cứu cũng góp phần vào việc xây dựng và hoàn thiện hệ thống lý luận về nhóm tội phạm trong lĩnh vực CNTT và mạng viễn thông.

#### **Tài liệu tham khảo**

1. Bộ luật Hình sự năm 1999.
2. Bộ luật Hình sự năm 2015, sửa đổi bổ sung năm 2017.
3. Tòa án nhân dân tối cao, *Báo cáo tình hình tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông*, Hà Nội, 2020.
4. Viện Khoa học Pháp lý - Bộ Tư pháp, *Nghiên cứu tính thống nhất giữa Bộ luật hình sự trong việc quy định các tội phạm với các luật khác trong hệ thống pháp luật Việt Nam*, tháng 9/2016.
5. Nguyễn Ngọc Hòa, *Bình luận khoa học Bộ luật hình sự năm 2015, được sửa đổi, bổ sung năm 2017* (phần các tội phạm), quyển 2, NXB Tư pháp, Hà Nội, 2018.
6. Viện Khoa học Pháp lý, *Từ điển luật học*, NXB Từ điển Bách khoa - NXB Tư pháp, Hà Nội, 2006.
7. Nguồn: <https://www.toaan.gov.vn/>