NGUYỄN VĂN MINH - PHÁP LUẬT

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

==========

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

==========

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Tình huống 1: Để kiếm thêm thu nhập, bạn Minh, Lan và Hùng là 3 sinh viên mới ra trường cùng có ý tưởng kinh doanh thương mại điện tử. Cả 3 quyết định cùng lập trang Web bán hàng trực tuyến "MuaSam.com", nhóm bán hàng với các sản phẩm giảm giá từ 20% đến 40%. Ngay ngày hôm sau, Website "Muasam.com" được thiết lập. Thực hiện ý tưởng của mình, nhóm đã tiến hành gặp gỡ và đàm phán với các doanh nghiệp cung ứng hàng hoá, dịch vụ được giảm giá. Khách hàng muốn mua hàng sẽ sử dụng dịch vụ được đăng lên Website "Muasam.com" thực hiện đặt hàng trực tuyến, khách hàng có thể thực hiện thanh toán trực tuyến hoặc thanh toán tại nhà, nếu có voucher khách hàng sẽ click chọn nhận voucher và nhận mã giảm giá, khách hàng nhập mã giảm giá của voucher. Sau khi đặt hàng khách hàng sẽ nhận thông báo xác nhận thông tin đặt hàng của mình cũng như thời gian sẽ giao hàng.

(1) Dựa vào các bô luật bạn đã học, hãy chỉ ra nhóm đã vi phạm khoản nào của điều khoản nào trong bộ luật nào? Trình bày nội dung điều khoản luật đó
(2) Nếu bạn là nhóm trên thì bạn sẽ phải làm gì để không vi phạm các điều khoản luật mà vẫn đạt được mục tiêu đặt ra.
(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự nhóm trên ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

Phân tích tình huống vi phạm pháp luật về thương mại điện tử

1. Các điều khoản pháp luật bị vi phạm

- **Khoản 1 Điều 27 Nghị định 52/2013/NĐ-CP (về thương mại điện tử)**: Quy định **thương nhân, tổ chức, cá nhân lập website thương mại điện tử bán hàng phải thông báo với Bộ Công Thương về việc thiết lập website đó**. Trong tình huống, nhóm đã tự ý lập trang web "MuaSam.com" mà **không thông báo với Bộ Công Thương**, nên đã vi phạm quy định này.
- **Khoản 1 Điều 28 Nghị định 52/2013/NĐ-CP**: Yêu cầu **website thương mại điện tử bán hàng phải cung cấp đầy đủ thông tin** về chủ sở hữu website, về hàng hóa/dịch vụ và các điều khoản hợp đồng mua bán áp dụng cho sản phẩm trên website. Nhóm sinh viên đã **không công bố đầy đủ thông tin bắt buộc** trên "MuaSam.com" (như thông tin người sở hữu, địa chỉ liên hệ, chính sách giao dịch...), do đó vi phạm nghĩa vụ cung cấp thông tin theo Điều 28.
- **Khoản 2 Điều 9 Luật Công nghệ thông tin 2006**: Quy định **tổ chức, cá nhân kinh doanh trên môi trường mạng phải thông báo công khai trên mạng các thông tin liên quan**, bao gồm: tên, địa chỉ, số điện thoại, email; thông tin về đăng ký kinh doanh hoặc quyết định thành lập (nếu có); tên cơ quan quản lý (nếu có); thông tin về giá, thuế, phí (nếu có). Nhóm đã **không đăng tải công khai các thông tin pháp lý và liên hệ bắt buộc** này trên website, vi phạm Khoản 2 Điều 9 Luật CNTT 2006.
- **Khoản 1 Điều 21 Luật Công nghệ thông tin 2006**: Quy định **chỉ được thu thập, xử lý, sử dụng thông tin cá nhân của người khác khi được người đó đồng ý**, trừ trường hợp pháp luật có quy định khác. Trên website "MuaSam.com", khách hàng phải nhập thông tin cá nhân (để đặt hàng, nhận voucher...). Nếu trang web **không có cơ chế cho khách hàng xác nhận đồng ý về việc thu thập và mục đích sử dụng thông tin cá nhân**, thì nhóm đã vi phạm Điều 21 (Khoản 1) Luật CNTT về bảo vệ dữ liệu cá nhân.
- **Khoản 2 Điều 21 Luật Công nghệ thông tin 2006**: Quy định **trách nhiệm của bên thu thập thông tin cá nhân**, cụ thể: **(a)** phải thông báo cho người đó về **hình thức, phạm vi, địa điểm, mục đích** thu thập và sử dụng thông tin; **(b)** chỉ **sử dụng đúng mục đích** thông tin thu thập và **chỉ lưu trữ trong thời gian cần thiết**; **(c)** áp dụng **biện pháp kỹ thuật, quản lý** để bảo đảm thông tin cá nhân không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá huỷ. Nhóm chưa xây dựng chính sách bảo mật hay biện pháp bảo vệ dữ liệu trên website, không thông báo mục đích thu thập dữ liệu cho khách, tức là **không thực hiện các trách nhiệm (a), (b), (c)** nêu trên – vi phạm Khoản 2 Điều 21 Luật CNTT 2006.
- **Điều 17 Luật An toàn thông tin mạng 2015**: Quy định về **thu thập và sử dụng thông tin cá nhân trên mạng**. Theo đó, **chỉ được thu thập thông tin cá nhân sau khi có sự đồng ý của chủ thể thông tin về phạm vi và mục đích sử dụng**; không được sử dụng thông tin cá nhân vào mục đích khác hoặc **cung cấp cho bên thứ ba khi chưa được sự đồng ý của chủ thể thông tin**. Nhóm đã thu thập thông tin khách hàng (cho việc mua hàng,

nhận voucher) **mà chưa có cơ chế xin phép khách hàng về phạm vi, mục đích sử dụng**, vi phạm quy định tại Điều 17 Luật ATTTM 2015.

- **Điều 19 Luật An toàn thông tin mạng 2015**: Quy định **tổ chức, cá nhân thu thập thông tin cá nhân phải áp dụng biện pháp quản lý, kỹ thuật phù hợp để bảo vệ thông tin cá nhân** mà mình thu thập, lưu trữ. Website "MuaSam.com" chưa có biện pháp bảo mật (như mã hóa thông tin thanh toán, chính sách bảo vệ dữ liệu...), tức là **chưa tuân thủ yêu cầu bảo đảm an toàn thông tin cá nhân** theo Điều 19 Luật ATTTM 2015.

*(Ngoài ra, nhóm có thể vi phạm các quy định khác như: **Luật Doanh nghiệp** về đăng ký kinh doanh (nếu chưa đăng ký mà đã hoạt động thương mại), hoặc pháp luật **về thuế** (nếu chưa kê khai nộp thuế cho doanh thu bán hàng). Tuy nhiên, các vi phạm chính trong tình huống này tập trung vào lĩnh vực thương mại điện tử và an toàn thông tin mạng như trên.)*

2. Biện pháp khắc phục để không vi phạm pháp luật và vẫn đạt mục tiêu

Nếu là nhóm Minh, Lan, Hùng, để kinh doanh hiệu quả mà **không vi phạm pháp luật**, cần thực hiện các biện pháp sau:

- **Đăng ký và thông báo theo quy định**: Trước khi hoạt động, nhóm nên **đăng ký kinh doanh** (thành lập doanh nghiệp hoặc hộ kinh doanh cá thể) và **thông báo website thương mại điện tử với Bộ Công Thương** theo thủ tục Nghị định 52/2013. Việc này giúp hợp pháp hóa website "MuaSam.com" và tránh bị xử phạt hành chính.
- **Công khai đầy đủ thông tin trên website**: Đảm bảo trang web hiển thị rõ **thông tin về chủ sở hữu** (tên công ty/cá nhân, địa chỉ, điện thoại, email), **số đăng ký kinh doanh hoặc quyết định thành lập**, **cơ quan quản lý** (nếu có), cùng các **điều kiện giao dịch** (giá cả đã gồm thuế/phí, chính sách vận chuyển, đổi trả, bảo hành, thanh toán). Những thông tin này phải **rõ ràng, dễ tìm** để tuân thủ Nghị định 52 và Luật CNTT, đồng thời tạo sự tin cậy cho khách hàng.
- **Xây dựng quy chế hoạt động và giải quyết khiếu nại**: Thiết lập trên website **các điều khoản sử dụng, chính sách mua bán, bảo mật và cơ chế giải quyết tranh chấp**. Ví dụ: quy định phương thức tiếp nhận và xử lý **khiếu nại của khách hàng**, điều khoản về **bảo hành, đổi trả**, và khuyến khích **hòa giải tranh chấp** trực tuyến nếu có mâu thuẫn. Điều này vừa đáp ứng yêu cầu pháp lý (theo tinh thần Luật Giao dịch điện tử 2005 về giải quyết tranh chấp), vừa giúp nhóm giữ uy tín với khách.
- **Bảo vệ thông tin cá nhân và an toàn thanh toán**: Thực hiện **chính sách bảo mật** theo Luật ATTTM. Cụ thể, **xin sự đồng ý của người dùng trước khi thu thập thông tin cá nhân**, thông báo rõ mục đích sử dụng; **chỉ dùng thông tin đúng mục đích, không chia sẻ cho bên thứ ba khi chưa được phép**. Về kỹ thuật, cần **mã hóa dữ liệu khách hàng**, sử dụng giao thức **HTTPS** cho website, hợp tác với cổng thanh toán uy tín (thay vì tự lưu trữ thông tin thẻ thanh toán) để **đảm bảo an toàn giao dịch**. Các biện pháp này tuân thủ Điều 19 Luật ATTTM (bảo vệ thông tin cá nhân) và giúp khách hàng yên tâm mua sắm.

- **Tuân thủ quy định về khuyến mại và voucher**: Nếu triển khai chương trình giảm giá 20%-40% qua voucher, nhóm cần **ký hợp đồng rõ ràng với nhà cung cấp** về việc giảm giá, và **đăng ký chương trình khuyến mại với cơ quan chức năng** (Sở Công Thương) nếu luật yêu cầu. Như vậy sẽ **vừa giữ được ưu đãi cho khách hàng, vừa không vi phạm pháp luật về thương mại** (Luật Thương mại về xúc tiến thương mại).

Tóm lại, nhóm cần tích cực **hoàn thiện các thủ tục pháp lý và biện pháp kỹ thuật** nêu trên ngay từ đầu. Điều này giúp dự án **đạt mục tiêu kinh doanh** (thu hút khách hàng, tăng thu nhập) **mà không vi phạm pháp luật**, đồng thời tạo nền tảng uy tín cho sự phát triển lâu dài.

3. Thực trạng vi phạm tương tự ở Việt Nam và giải pháp hạn chế

Thực trạng chung: Vi phạm pháp luật trong thương mại điện tử như tình huống trên **khá phổ biến** ở Việt Nam. Nhiều cá nhân, nhóm khởi nghiệp **bán hàng online** nhưng **không đăng ký, thông báo website** theo quy định. Không ít website thương mại điện tử **không công khai đầy đủ thông tin** về doanh nghiệp, hoặc hoạt động dưới danh nghĩa cá nhân để trốn tránh nghĩa vụ thuế và trách nhiệm pháp lý. Việc **thu thập và sử dụng thông tin khách hàng tùy tiện** cũng rất thường gặp – ví dụ: nhiều trang web yêu cầu người dùng cung cấp dữ liệu cá nhân nhưng **không có chính sách bảo mật, không xin phép người dùng**, sau đó có thể dùng dữ liệu cho mục đích quảng cáo hoặc bán cho bên thứ ba. Bên cạnh đó, **tình trạng bảo mật kém** dẫn đến rò rỉ thông tin khách hàng tại một số sàn thương mại điện tử đã xảy ra, do doanh nghiệp chưa tuân thủ chặt chẽ các tiêu chuẩn an toàn thông tin. Nguyên nhân của thực trạng này là **nhận thức pháp lý của người kinh doanh còn hạn chế**, cộng với việc **thanh tra, xử lý vi phạm trên môi trường mạng chưa thường xuyên, nghiêm minh**. Nhiều startup cho rằng thủ tục pháp lý rườm rà, hoặc **chủ quan** nghĩ rằng kinh doanh nhỏ lẻ thì nhà nước khó kiểm soát, dẫn đến vi phạm.

Giải pháp hạn chế: Để giảm thiểu các vi phạm tương tự, cần phối hợp nhiều biện pháp sau:

- **Tuyên truyền và hướng dẫn pháp luật:** Cơ quan quản lý (Bộ Công Thương, Bộ TT&TT,...) nên tăng cường **phổ biến quy định pháp luật về thương mại điện tử và an toàn thông tin**. Có thể tổ chức các **hội thảo, lớp tập huấn** cho doanh nghiệp khởi nghiệp, phát hành **cẩm nang hướng dẫn** các bước cần làm khi lập website bán hàng. Khi người kinh doanh **hiểu rõ nghĩa vụ** và lợi ích của việc tuân thủ pháp luật, họ sẽ chủ động chấp hành hơn.
- **Đơn giản hóa thủ tục, hỗ trợ doanh nghiệp:** Nhà nước cần tiếp tục **đơn giản hóa quy trình thông báo, đăng ký website** (thực hiện online nhanh chóng, miễn phí) để startup dễ thực hiện. Đồng thời thiết lập **kênh hỗ trợ** (đường dây nóng, cổng thông tin) tư vấn cho doanh nghiệp mới về các quy định TMĐT. Nếu thủ tục **thuận tiện** và doanh nghiệp được **hỗ trợ tận tình**, họ sẽ **ít động cơ vi phạm** hơn.
- **Tăng cường kiểm tra, xử phạt nghiêm minh:** Cơ quan chức năng cần **thanh tra định kỳ** các website, sàn giao dịch TMĐT. Những trường hợp như **không thông báo website, không cung cấp thông tin đầy đủ, vi phạm bảo mật**... phải bị **xử phạt nghiêm** theo Nghị định 98/2020/NĐ-CP (về xử phạt TMĐT) và các văn bản liên quan. Việc công khai

các trường hợp bị xử phạt sẽ tạo **tính răn đe**, cảnh báo các chủ thể khác tuân thủ pháp luật tốt hơn.

- **Áp dụng tiêu chuẩn an toàn thông tin:** Khuyến khích và hỗ trợ doanh nghiệp TMĐT **áp dụng các tiêu chuẩn bảo mật** (như tiêu chuẩn **PCI-DSS** trong thanh toán thẻ, **ISO/IEC 27001** về quản lý an ninh thông tin). Nhà nước có thể ban hành hướng dẫn cụ thể và yêu cầu các sàn TMĐT lớn phải tuân thủ tiêu chuẩn kỹ thuật bảo vệ dữ liệu người dùng. Mặt khác, cần **phối hợp với các chuyên gia an ninh mạng** để giúp doanh nghiệp nhỏ nâng cấp hệ thống bảo mật, phòng chống tấn công mạng, qua đó **bảo vệ thông tin khách hàng** và tuân thủ luật ATTTM.
- **Nâng cao ý thức tự giác của doanh nghiệp:** Về lâu dài, mỗi cá nhân, doanh nghiệp kinh doanh online phải **tự ý thức tuân thủ pháp luật**. Hiểu rằng **tuân thủ quy định không chỉ để tránh bị phạt**, mà còn tạo môi trường kinh doanh lành mạnh và **uy tín cho chính doanh nghiệp**. Khi doanh nghiệp **bán hàng minh bạch, bảo vệ tốt dữ liệu và quyền lợi khách hàng**, họ sẽ chiếm được lòng tin và trung thành của khách, từ đó kinh doanh bền vững hơn.

Tình huống 2: Hơn 14.000 điện thoại ở Việt Nam đã bị một công ty tư nhân nghe lén. Các điện thoại này bị theo dõi tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh... Nghiêm trọng hơn, toàn bộ dữ liệu được gửi về máy chủ của công ty này. Kết quả thanh tra đã khiến người sử dụng điện thoại ở Việt Nam cảm thấy lo lắng. Đoàn thanh tra liên ngành gồm thanh tra Sở Thông tin và Truyền thông Hà Nội, phòng Cảnh sát phòng chống tội phạm sử dụng công nghệ cao - PC50 của Công an Hà Nội đã thanh tra tại công ty TNHH công nghệ Việt Hồng ở quận Thanh Xuân, Hà Nội và phát hiện công ty này kinh doanh phần mềm Ptraker. Đây là phần mềm giúp người dùng có thể xem tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh, bật - tắt 3G/GPRS của điện thoại bị giám sát. Thậm chí người sử dụng còn có thể ra lệnh điều khiển từ xa điện thoại bị cài Ptracker bằng cách nhắn tin tới điện thoại này.

(1) Dựa vào các bộ luật bạn đã học, hãy chỉ ra công ty trên đã vi phạm khoản nào của điều khoản nào trong bộ luật nào? Trình bày nội dung điều khoản luật đó.

(2) Hãy bạn hiểu như thế nào về điều khoản luật này? Nếu bạn là chủ doanh nghiệp thì bạn sẽ giải quyết định gì về phần mềm này.

(3) Bạn hãy tìm hiểu và trình bày hiện nay có những phần mềm/trang mạng xã hội nào mà thông tin cá nhân người dùng có thể bị sử dụng bất hợp pháp?

Pháp lý về hành vi nghe lén điện thoại

1. Điều luật bị vi phạm

Hành vi gián điệp điện thoại của Công ty Việt Hồng vi phạm nghiêm trọng quy định pháp luật về bảo vệ thông tin cá nhân và an toàn thông tin mạng. Cụ thể, theo **Luật An ninh mạng 2018**, Điều 17

Khoản 1 mục đ (đ) quy định: *"Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại"* là hành vi bị nghiêm cấm. Phần mềm Ptracker cho phép nghe lén và ghi âm cuộc gọi từ xa, do đó đã vi phạm trực tiếp quy định này. Ngoài ra, theo **Luật Công nghệ thông tin 2006**, Điều 71 Khoản 1 quy định cấm tổ chức, cá nhân tạo ra, cài đặt hoặc phát tán phần mềm độc hại nhằm thực hiện hành vi thu thập trái phép thông tin cá nhân của người khác. Phần mềm Ptracker rõ ràng là phần mềm gián điệp ("phần mềm gây hại") được sử dụng để thu thập tin nhắn, danh bạ, định vị... nên vi phạm Điều 71. Hơn nữa, **Luật An toàn thông tin mạng 2015** (Luật ATTTM), Điều 7 Khoản 1 mục 5 cũng nghiêm cấm "thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác". Việc thu thập tràn lan tin nhắn, ghi âm, hình ảnh riêng tư của hơn 14.000 thuê bao mà không được phép chủ thuê bao chính là vi phạm điều khoản này.

Tóm lại, hành vi nghe lén của Công ty Việt Hồng vi phạm ít nhất các quy định: **Luật An ninh mạng 2018** (Điều 17(1)(đ) về gián điệp mạng)vbpl.vn, **Luật Công nghệ thông tin 2006** (Điều 71) và **Luật An toàn thông tin mạng 2015** (Điều 7(1)(5)).

2. Ý nghĩa điều luật và xử lý phần mềm

- **Ý nghĩa quy định pháp luật:** Các điều luật trên đều nhằm bảo vệ quyền riêng tư và an toàn thông tin của cá nhân. Ví dụ, Điều 17 Luật An ninh mạng 2018 coi việc nghe lén, ghi âm trái phép là một hình thức gián điệp mạng, xâm phạm quyền lợi hợp pháp của cá nhân và tổ chức, do đó bị nghiêm cấmvbpl.vn. Tương tự, Luật CNTT 2006 yêu cầu không tạo ra hay phát tán phần mềm độc hại để thu thập thông tin cá nhân, nhấn mạnh rằng mọi thông tin cá nhân thu thập trên môi trường mạng phải được người dùng đồng ý. Thực tế, Điều 21 Luật CNTT 2006 quy định tổ chức, cá nhân chỉ được thu thập, xử lý thông tin cá nhân khi đã được chủ sở hữu cho phép. Những quy định này khẳng định mục đích bảo vệ bí mật cá nhân, hạn chế tội phạm công nghệ cao và ngăn chặn gián điệp mạng.
- **Xử lý phần mềm với tư cách chủ doanh nghiệp:** Nếu tôi là chủ doanh nghiệp, tôi sẽ xử lý Ptracker như phần mềm gián điệp bị cấm. Trước hết, phải dừng ngay mọi hoạt động phân phối hoặc sử dụng Ptracker vì nó vi phạm pháp luật. Tôi sẽ thu hồi và vô hiệu hóa phần mềm này để đảm bảo tuân thủ luật pháp. Đồng thời, cần báo cáo với cơ quan chức năng về việc kinh doanh phần mềm trái phép và phối hợp khắc phục hậu quả (như thông báo tới người dùng bị xâm phạm). Theo Luật CNTT, doanh nghiệp phải đảm bảo việc thu thập thông tin cá nhân phải minh bạch và có sự đồng ý của người dùng; nếu không sẽ bị xử phạt. Tôi cũng phải rà soát lại toàn bộ phần mềm, áp dụng giải pháp an ninh chặt chẽ hơn và chỉ sử dụng phần mềm có bản quyền, rõ nguồn gốc. Ngoài ra, tôi cần tư vấn pháp lý để xây dựng quy trình bảo mật thông tin và đào tạo nhân viên về luật an ninh mạng, nhằm không vi phạm các điều khoản tương tự trong tương lai.

3. Các phần mềm và mạng xã hội có nguy cơ vi phạm

– **Mạng xã hội:** Nhiều mạng xã hội lớn có nguy cơ thu thập hoặc để lộ thông tin cá nhân người dùng. Ví dụ, Facebook đã gặp nhiều bê bối về rò rỉ dữ liệu cá nhân. Báo cáo cho thấy tại Việt Nam có đến 427.446 tài khoản Facebook bị lộ thông tin cá nhân (xếp thứ 9 thế giới). Các mạng xã hội khác như

Instagram, TikTok, Twitter cũng thu thập dữ liệu người dùng và có nguy cơ bị sử dụng bất hợp pháp nếu không được bảo mật đúng quy định.

– **Ứng dụng di động, thương mại điện tử:** Nhiều ứng dụng yêu cầu quyền truy cập thông tin cá nhân để cung cấp dịch vụ (thương mại điện tử, ngân hàng, bảo hiểm, đặt vé,...). Ví dụ, để mua bán hàng hoặc thanh toán trực tuyến, người dùng phải cung cấp rất nhiều dữ liệu riêng tư (số điện thoại, địa chỉ, tài khoản ngân hàng...). Nếu các ứng dụng này không tuân thủ quy định lưu trữ, bảo vệ dữ liệu (như bắt buộc lưu trữ dữ liệu người dùng tại Việt Nam theo Điều 26.3 Luật An ninh mạng 2018) hoặc sử dụng thông tin sai mục đích thì nguy cơ vi phạm luật là rất cao. Các phần mềm chat/messaging (Zalo, Viber, WhatsApp) hoặc game online cũng tiềm ẩn rủi ro thu thập dữ liệu riêng tư.

– **Các phần mềm khác:** Ngoài ra, các phần mềm gián điệp như Ptracker, các ứng dụng theo dõi điện thoại (spyware) hoặc công cụ camera, ghi âm không rõ nguồn gốc cũng có nguy cơ cao vi phạm. Các chương trình này thường xâm nhập thiết bị của người dùng để thu thập dữ liệu bí mật (tin nhắn, cuộc gọi, hình ảnh...) mà không có sự đồng ý, vi phạm quy định Luật CNTT về bảo vệ thông tin cá nhân.

Tình huống 3: Để kiếm thêm thu nhập, bạn A đã tự tạo ra một website thương mại điện tử để bán thêm các quần áo, đồ dùng cá nhân, mỹ phẩm, thực phẩm chức năng,... được chị của bạn A xách tay từ Nhật. Bạn A không đăng ký giấy phép kinh doanh cũng như đăng ký webite với cơ quan có thẩm quyền. Ngoài ra, các hình ảnh quảng cáo các sản phẩm, bạn A vào các trang web khác lấy về và đăng tải lên trang thương mại điện tử của mình.

(1) Dựa vào các bô luật bạn đã học, hãy chỉ ra bạn A đã vi phạm khoản nào của điều khoản nào trong bộ luật nào? Trình bày nội dung điều khoản luật đó

(2) Nếu bạn là bạn A thì bạn sẽ phải làm gì để không vi phạm các điều khoản luật mà vẫn đạt được mục tiêu đặt ra.

(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự A ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

(1) Vi phạm pháp luật

Bạn A đã vi phạm nhiều quy định pháp luật hiện hành về thương mại điện tử và sở hữu trí tuệ. Cụ thể:

- **Không thông báo website với Bộ Công Thương:** Theo Nghị định 52/2013/NĐ-CP (quy định về thương mại điện tử), Điều 27 khoản 1 quy định: "*Thông báo với Bộ Công Thương về việc thiết lập website thương mại điện tử bán hàng theo quy định tại mục 1 Chương IV Nghị định này*". Việc A tự lập website bán hàng mà không thực hiện thủ tục thông báo với Bộ Công Thương đã vi phạm khoản này.
- **Không đăng ký kinh doanh:** Luật Công nghệ thông tin (2006) yêu cầu tổ chức, cá nhân kinh doanh trên mạng phải công khai thông tin giấy phép đăng ký kinh doanh (nếu có). Cụ thể, Khoản 2 Điều 9 Luật Công nghệ thông tin quy định người kinh doanh trên môi

trường mạng phải công khai *"giấy chứng nhận đăng ký kinh doanh (nếu có)"*. A không đăng ký giấy phép kinh doanh nên không niêm yết được thông tin này, vi phạm quy định công khai thông tin kinh doanh trên mạng.

- **Xâm phạm bản quyền hình ảnh:** Việc A sao chép hình ảnh quảng cáo của trang khác rồi đăng lên website là hành vi vi phạm quyền tác giả. Luật Sở hữu trí tuệ (2005) tại Điều 28 khoản 3 quy định: "*Công bố, phân phối tác phẩm mà không được phép của tác giả*" là xâm phạm quyền tác giả. Hình ảnh quảng cáo được xem là tác phẩm nhiếp ảnh hoặc mỹ thuật ứng dụng được bảo hộ (Điều 14 Luật SHTT), nên việc A sử dụng mà không xin phép tác giả là vi phạm Luật SHTT.

Như vậy, A đã vi phạm ít nhất các quy định: Điều 27 Khoản 1 Nghị định 52/2013 (thương mại điện tử), Điều 9 Khoản 2(b) Luật Công nghệ thông tin và Điều 28 Khoản 3 Luật Sở hữu trí tuệ. Các nội dung điều khoản trên đều cấm các hành vi mà A đang thực hiện.

(2) Biện pháp để tuân thủ pháp luật

Nếu là A, để vừa kinh doanh vừa tuân thủ pháp luật, cần thực hiện các bước sau:

- **Đăng ký kinh doanh hợp pháp:** Trước hết, A nên đăng ký giấy phép kinh doanh (ví dụ dưới hình thức hộ kinh doanh cá thể hoặc doanh nghiệp) theo quy định Luật Doanh nghiệp và Thương mại. Việc này vừa hợp pháp hoá hoạt động kinh doanh, vừa tạo thuận lợi cho nghĩa vụ thuế. Đồng thời, A phải công bố công khai thông tin này trên website, như yêu cầu của Luật Công nghệ thông tin (Điều 9, Khoản 2(b)).
- **Thông báo với Bộ Công Thương về website TMĐT:** A cần tiến hành thủ tục thông báo website TMĐT với Bộ Công Thương theo quy định tại Khoản 1 Điều 27 Nghị định 52/2013. Sau khi thông báo, website được cấp mã số và A sẽ hoàn thành nghĩa vụ đăng ký pháp lý cho hoạt động TMĐT.
- **Cung cấp đầy đủ thông tin trên website:** Theo Điều 28 Nghị định 52/2013, website TMĐT bán hàng phải "cung cấp đầy đủ thông tin về người sở hữu website, hàng hóa, dịch vụ và các điều khoản của hợp đồng mua bán...". A cần chỉnh sửa website để hiển thị rõ tên chủ sở hữu (công ty hoặc cá nhân), địa chỉ, giấy phép kinh doanh, thông tin sản phẩm, giá cả kèm thuế, chi phí vận chuyển... nhằm tuân thủ quy định này.
- **Dùng hình ảnh có bản quyền hoặc tự chụp:** Để không vi phạm bản quyền, A không nên sử dụng ảnh của người khác mà không có phép. Thay vào đó, A có thể tự chụp ảnh sản phẩm hoặc mua/bản quyền ảnh từ các nguồn hợp pháp. Việc này vừa tôn trọng quyền tác giả (tránh vi phạm Điều 28 Khoản 3 Luật SHTT), vừa nâng cao uy tín kinh doanh.
- **Thực hiện đầy đủ nghĩa vụ khác:** A cũng cần nhớ thực hiện các nghĩa vụ pháp lý khác như nộp thuế theo quy định (Điều 27.7 NĐ 52/2013 yêu cầu thực hiện đầy đủ nghĩa vụ thuế) và tuân thủ các quy định quảng cáo, an toàn thông tin (nếu có) để kinh doanh bền vững.

Nếu thực hiện đủ các biện pháp trên (đăng ký kinh doanh, thông báo website, hiển thị thông tin minh bạch, dùng ảnh hợp pháp), A sẽ vừa đạt được mục tiêu kinh doanh trực tuyến vừa không vi phạm pháp luật hiện hành.

(3) Nhận xét chung và giải pháp đề xuất

Tình trạng như của A (bán hàng online chưa đăng ký và sử dụng ảnh không phép) khá phổ biến ở Việt Nam hiện nay. Theo tài liệu học tập, **"hiện nay, tình trạng vi phạm sở hữu trí tuệ ở nước ta vẫn đang ở mức báo động"**. Với sự phát triển của thương mại điện tử, nhiều cá nhân, hộ kinh doanh nhỏ lẻ chỉ đăng bán online mà không đăng ký giấy phép hay tuân thủ quy định pháp luật; đồng thời họ dễ dàng sao chép, tái sử dụng ảnh và nội dung mà không có bản quyền. Điều này gây bất lợi cho cả người tiêu dùng (thông tin không rõ ràng, kém tin cậy) và thị trường chân chính (tổn hại quyền tác giả, cạnh tranh không lành mạnh).

Để giảm thiểu vi phạm, một số giải pháp có thể áp dụng:

- **Tăng cường tuyên truyền và hướng dẫn:** Chính phủ và các cơ quan chức năng cần đẩy mạnh tuyên truyền về quy định pháp luật cho các cá nhân kinh doanh online (ví dụ tổ chức hội thảo, hướng dẫn trực tuyến). Cung cấp tài liệu, mẫu hướng dẫn cho việc đăng ký kinh doanh và thông báo website sẽ giúp người kinh doanh hiểu rõ thủ tục bắt buộc.
- **Giảm thủ tục hành chính:** Đơn giản hóa thủ tục đăng ký kinh doanh cá thể và thông báo website TMĐT (trực tuyến, trả kết quả nhanh) sẽ khuyến khích người bán tuân thủ hơn. Ví dụ, liên thông hệ thống kê khai thuế và đăng ký online giúp tiết kiệm thời gian.
- **Tăng cường kiểm tra, xử phạt:** Đẩy mạnh thanh tra, giám sát hoạt động TMĐT, xử lý nghiêm các trường hợp vi phạm (theo Nghị định xử phạt vi phạm hành chính trong lĩnh vực thương mại điện tử). Hình phạt hành chính hay cấm quảng cáo có thể răn đe các đơn vị chây ỳ, như quy định xử phạt xây dựng website mà không thông báo Bộ Công Thương.
- **Hỗ trợ về bản quyền ảnh:** Khuyến khích người kinh doanh sử dụng ảnh miễn phí bản quyền hoặc mua ảnh có phép bằng cách giới thiệu các kho ảnh hợp pháp (Creative Commons, Shutterstock, iStock...) và giải thích hậu quả pháp lý khi dùng ảnh lậu. Các khóa học, hướng dẫn trực tuyến về bảo vệ SHTT có thể nâng cao nhận thức rằng "sao chép, quảng bá nội dung... ngày càng dễ dàng" nhưng hành vi này là vi phạm pháp luật.
- **Nâng cao trách nhiệm của nền tảng TMĐT:** Các sàn thương mại điện tử lớn nên yêu cầu thành viên khai báo giấy phép kinh doanh khi mở gian hàng, và kiểm duyệt nội dung quảng cáo (yêu cầu hình ảnh phải có bản quyền hoặc do chính cửa hàng tự chụp).

Tóm lại, để ngăn chặn vi phạm tương tự, cần kết hợp giữa tuyên truyền pháp luật, cải cách thủ tục, chế tài xử lý và nâng cao ý thức người kinh doanh. Điều này sẽ tạo ra môi trường TMĐT minh bạch, đảm bảo quyền lợi cho người tiêu dùng và người sản xuất chân chính.

Tình huống 4: Một sinh viên ngành CNTT rất đam mê công việc của một bác sĩ máy tính chuyên cứu hộ các máy tính bị tấn công bởi các mã độc, phân tích các mối đe dọa của một hệ thống thông tin để từ đó cài đặt các cơ chế phù hợp để giảm thiểu các rũi ro cho hệ thống thông tin đó. Vì vậy, sinh viên này thường xuyên vào các diễn dàn để tìm hiểu, học hỏi các kỹ thuật tấn công, các mã độc, các kỹ thuật tìm kiếm các lỗ hỏng của các công nghệ,... Sau đó thực hiện thử nghiệm hết tất cả các kỹ thuật đã học hỏi vào bất cứ hệ thống thông tin bất kỳ mà mình thích. Kết quả đến nay đã thử nghiệm thành công rất nhiều công cụ và kỹ thuật đã học hỏi và làm nhiều máy tính, cũng như website của nạn nhân lao đao vì các thử nghiệm này. Ngoài ra trong một lần tấn công thử nghiệm, người này đã sao chép được rất nhiều thông tin bảo mật của hệ thống này. Sau đó người này đem các thông tin này đăng tải lên các diễn đàn công cộng như là chiến tích của cá nhân mình.

(1) Dựa vào Bộ luật an ninh mạng, bạn hãy chỉ ra sinh viên trong tình huống trên **đã vi phạm những khoản nào** trong bộ luật? Trình bày nội dung điều khoản luật đó ra.

(2) Bạn hãy **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Giả sử bạn là nhân viên làm việc trong ngành CNTT, bạn hãy **đưa ra và giải thích ít nhất 3 lý do** tại sao bạn cần nắm rõ các một số điều khoản luật trong luật an ninh mạng.

Phân tích quy định pháp luật liên quan đến hành vi tấn công hệ thống

Dựa trên Luật An toàn thông tin mạng (2015) và Luật Công nghệ thông tin (2006) trong tài liệu đã cho, sinh viên nêu trên đã vi phạm các điều khoản sau:

- **Luật An toàn thông tin mạng (ATTTM) – Điều 4, Khoản 2:** *"Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác."*.
- **Luật ATTTM – Điều 7, Khoản 1:** *"Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật."*.
- **Luật ATTTM – Điều 7, Khoản 3:** *"Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin."*.
- **Luật Công nghệ thông tin (CNTT) 2006 – Điều 12, Khoản 2:** *"Cản trở hoạt động hợp pháp hoặc hỗ trợ hoạt động bất hợp pháp về ứng dụng và phát triển công nghệ thông tin; ... phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng."*.

Trên đây là các điều khoản luật có nội dung trùng khớp với hành vi của sinh viên (xâm nhập, tấn công hệ thống và sao chép, phát tán dữ liệu mà không có quyền). Tiếp theo sẽ phân tích chi tiết ý nghĩa của từng quy định này.

Phân tích nội dung các điều khoản bị vi phạm

1. Điều 4, Khoản 2 Luật ATTTM: Điều này quy định nguyên tắc chung về trách nhiệm và giới hạn hành vi: *"Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân*

khác.”.
Cụ thể, quy định này cấm mọi hành vi can thiệp bất hợp pháp vào hệ thống thông tin của người khác. Nội dung này khẳng định rằng bất kỳ đối tượng nào – kể cả cá nhân hay tổ chức – đều không có quyền xâm nhập, truy cập hay thao tác trên hệ thống tin học của người khác mà chưa được phép. Trong tình huống trên, sinh viên đã “tấn công” và xâm nhập nhiều hệ thống, từ đó vi phạm nguyên tắc cơ bản này. Quy định nhằm bảo vệ tính toàn vẹn, riêng tư và quyền sở hữu dữ liệu cá nhân, cơ quan, tổ chức. Mọi hành vi trái phép đều bị coi là vi phạm luật.

2. Điều 7, Khoản 1 Luật ATTTM: Khoản này liệt kê các hành vi bị nghiêm cấm: *“Ngăn chặn việc truyền tải thông tin trên mạng, can thiệp, truy nhập, gây nguy hại, xóa, thay đổi, sao chép và làm sai lệch thông tin trên mạng trái pháp luật.”*.
Ở đây, nhiều khái niệm liên quan đến hành vi tấn công mạng được nêu ra. Đặc biệt, cụm từ *“xóa, thay đổi, sao chép … trái pháp luật”* bao hàm hành vi sao chép hoặc chiếm đoạt dữ liệu mà không có quyền. Đồng thời, hành vi “can thiệp, truy nhập, ngăn chặn … thông tin trên mạng” cũng được cấm. Trong tình huống cho sẵn, sinh viên đã truy nhập trái phép nhiều hệ thống và sao chép dữ liệu bảo mật để công bố. Như vậy, sinh viên đã thực hiện cả hành vi *“truy nhập”* và *“sao chép thông tin … trái pháp luật”* theo quy định, vi phạm nghiêm trọng Điều 7 khoản 1. Mục đích của điều này là bảo đảm thông tin trên mạng luôn có độ tin cậy, nguyên vẹn, tránh bị đe dọa hay bị lạm dụng.

3. Điều 7, Khoản 3 Luật ATTTM: Khoản này tiếp tục liệt kê: *“Tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng của biện pháp bảo vệ an toàn thông tin mạng của hệ thống thông tin; tấn công, chiếm quyền điều khiển, phá hoại hệ thống thông tin.”*.
Nội dung khoản 3 nhấn mạnh tính nghiêm trọng của các cuộc tấn công mạng: cấm hoàn toàn việc phá hoại các biện pháp bảo vệ an toàn hoặc chiếm quyền điều khiển hệ thống. Sinh viên trong tình huống đã *“tấn công”* và gây ảnh hưởng nghiêm trọng đến nhiều hệ thống (một hình thức phá hoại biện pháp bảo vệ hoặc chiếm quyền điều khiển), nên hành vi này nằm trong các hành vi bị cấm nêu trên. Phần *“phá hoại hệ thống thông tin”* cho thấy mức độ vi phạm rất cao, có thể ảnh hưởng đến an toàn thông tin quốc gia hoặc của tổ chức cá nhân. Do đó, Khoản 3 Điều 7 quy định rõ những hành vi này là bất hợp pháp tuyệt đối.

4. Điều 12, Khoản 2 Luật CNTT 2006: Khoản này quy định các hành vi bị nghiêm cấm trong lĩnh vực CNTT. Theo đó: *“Cản trở hoạt động hợp pháp hoặc hỗ trợ hoạt động bất hợp pháp về ứng dụng và phát triển công nghệ thông tin; … phá hoại cơ sở hạ tầng thông tin, phá hoại thông tin trên môi trường mạng.”*.
Khổ điều này cấm mọi hành động can thiệp, phá hoại và hỗ trợ hoạt động bất hợp pháp trên môi trường số. Trong đó, *“phá hoại thông tin trên môi trường mạng”* tương đương với việc làm sai lệch, xóa hoặc công bố thông tin trái phép. Hành vi của sinh viên – tấn công hệ thống để đánh cắp dữ liệu bảo mật rồi công khai trên diễn đàn – chính là một dạng *“phá hoại cơ sở hạ tầng thông tin”* (bằng cách xâm nhập hệ thống và làm suy yếu an toàn) và *“phá hoại thông tin”* (bằng cách công bố thông tin bí mật). Hơn nữa, hành vi *“hỗ trợ hoạt động bất hợp pháp về ứng dụng CNTT”* cũng có thể xem xét nếu sinh viên chia sẻ kỹ thuật tấn công cho người khác. Như vậy, sinh viên đã vi phạm quy định tại

Điều 12 này, do đã thực hiện các hoạt động mạng bất hợp pháp ảnh hưởng xấu đến an toàn thông tin.

Lý do nhân viên CNTT cần nắm vững các quy định này

- **Tránh vi phạm pháp luật và chịu trách nhiệm hình sự:** Hiểu rõ các điều khoản quy định hành vi bị cấm giúp nhân viên CNTT tránh lầm lỗi. Nếu không nhận thức, một hành động "học hỏi kỹ thuật" có thể bị coi là xâm nhập trái phép và phải chịu xử lý hình sự. Nắm luật giúp chúng ta tự bảo vệ bản thân trước các tình huống pháp lý (vì *"không biết luật không tránh khỏi trách nhiệm"*).
- **Bảo vệ hệ thống và dữ liệu của tổ chức:** Nhân viên CNTT có trách nhiệm bảo mật hệ thống và thông tin. Biết rõ luật nghĩa là biết giới hạn được phép và không được làm gì. Ví dụ, hiểu rằng việc truy cập hay chia sẻ dữ liệu mà không có quyền là phạm luật sẽ giúp họ cảnh giác hơn, thực hiện biện pháp bảo vệ phù hợp, tránh rủi ro bị chính đồng nghiệp xâm nhập trái phép.
- **Nâng cao ý thức về đạo đức nghề nghiệp và uy tín ngành CNTT:** Khi hiểu các quy định, nhân viên CNTT biết mục đích của pháp luật là bảo vệ an ninh quốc gia và lợi ích công cộng. Điều này giúp họ tuân thủ các chuẩn mực đạo đức, không vì "hứng thú" hay tò mò mà thực hiện hành động trái phép. Nhờ đó, họ góp phần duy trì niềm tin và uy tín của nghề nghiệp, đồng thời bảo vệ khách hàng, tổ chức khỏi mất mát về thông tin.
- **Đáp ứng yêu cầu công việc và hợp tác với pháp luật:** Nhiều công việc CNTT yêu cầu triển khai hệ thống bảo mật tuân thủ pháp luật. Nhân viên hiểu rõ luật sẽ biết cách xây dựng quy trình, chính sách phù hợp. Đồng thời, khi có vụ việc vi phạm, họ cũng sẵn sàng phối hợp với cơ quan chức năng khai báo, xử lý đúng quy định, giúp khắc phục hiệu quả sự cố bảo mật.

Tình huống 5: Một website cung cấp dịch vụ giải trí miễn phí cho người dùng. Người dùng muốn truy cập vào các dịch vụ của website phải đăng ký tài khoản. Khi đăng ký tài khoản, người dùng phải cung cấp thông tin cá nhân như họ tên, địa chỉ nhà, email, số điện thoại.... Website không thông báo cho người dùng biết thông tin cá nhân của họ được dùng để làm gì. Website này thu thập thông tin người dùng để bán cho các nhà quảng cáo.

(1) Hãy cho biết hành vi của website trên có vi phạm pháp luật không? Nếu có, hãy cho biết hành vi trên vi phạm những điều khoản nào của những luật nào?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

Hành vi vi phạm và quy định pháp luật liên quan

Hành vi thu thập và sử dụng thông tin cá nhân của người dùng mà không thông báo mục đích và sau đó bán cho bên thứ ba rõ ràng vi phạm quy định về bảo vệ dữ liệu. Cụ thể, **Luật Công nghệ thông tin 2006** quy định tổ chức, cá nhân thu thập, xử lý thông tin cá nhân trên môi trường mạng "phải được người đó đồng ý". Trong tình huống trên, website không thông báo mục đích sử dụng khi yêu cầu cung cấp thông tin, tức không có sự đồng ý hợp lệ, vi phạm Khoản 1 Điều 21 Luật CNTT. Hơn nữa, theo Khoản 2 Điều 21 của Luật này, người thu thập thông tin phải **"thông báo cho người đó biết về hình thức, phạm vi, ... và mục đích của việc thu thập, xử lý và sử dụng thông tin cá nhân của người đó"**, và chỉ sử dụng thông tin đúng mục đích ban đầu cũng như bảo đảm an toàn dữ liệu. Việc website thu thập thông tin mà không thông báo mục đích (vi phạm Điều 21.2(a)), sau đó bán cho nhà quảng cáo (vi phạm việc sử dụng sai mục đích theo Điều 21.2(b)) là trái quy định.

Ngoài ra, **Luật An toàn thông tin mạng 2015** (Luật về An toàn thông tin mạng) cũng đặt ra trách nhiệm tương tự. Theo Điều 17 của Luật này, khi xử lý thông tin cá nhân tổ chức, cá nhân phải tiến hành thu thập sau khi có sự đồng ý và "thông báo cho chủ thể thông tin cá nhân về phạm vi, mục đích của việc thu thập và sử dụng"; đồng thời **cấm "cung cấp, chia sẻ, phát tán thông tin cá nhân đã thu thập... cho bên thứ ba" nếu không có sự đồng ý**. Việc website bán thông tin người dùng cho nhà quảng cáo là hành vi chuyển giao cho bên thứ ba mà không có sự đồng ý, vi phạm nghiêm trọng Khoản c Điều 17 này. Như vậy, hành vi nói trên vi phạm cả các quy định của Luật Công nghệ thông tin và Luật An toàn thông tin mạng về việc bảo vệ thông tin cá nhân.

Phân tích chi tiết điều khoản bị vi phạm

Luật Công nghệ thông tin 2006, Điều 21. Điều này chia làm hai phần chính. *Khoản 1* quy định bắt buộc phải có sự đồng ý của cá nhân trước khi thu thập thông tin cá nhân trên môi trường mạng. *Khoản 2* liệt kê nghĩa vụ của bên thu thập, trong đó:

- **Khoản 2(a)** quy định phải **"thông báo cho người đó biết về hình thức, phạm vi, địa điểm và mục đích của việc thu thập, xử lý và sử dụng thông tin cá nhân"**. Điều này nhằm đảm bảo người dùng hiểu rõ tại sao thông tin của họ được yêu cầu. Trong tình huống trên, website đã không thông báo mục đích sử dụng thông tin cá nhân, rõ ràng vi phạm nghĩa vụ này.
- **Khoản 2(b)** quy định bên thu thập chỉ được sử dụng thông tin đúng mục đích đã thông báo ban đầu và chỉ lưu trữ trong thời gian cần thiết. Việc website sử dụng thông tin để bán cho quảng cáo là nằm ngoài mục đích thu thập ban đầu (dịch vụ giải trí miễn phí) và chưa được sự đồng ý của người dùng, nên cũng vi phạm mục này.
- **Khoản 2(c)** yêu cầu **"tiến hành các biện pháp quản lý, kỹ thuật cần thiết để bảo đảm thông tin cá nhân không bị mất, đánh cắp, tiết lộ, thay đổi hoặc phá hủy"**. Hành vi chia sẻ – bán thông tin cho bên thứ ba cho thấy website không bảo mật dữ liệu hợp lý, vi phạm cả nguyên tắc này.

Luật An toàn thông tin mạng 2015, Điều 17. Luật này cụ thể hóa quy định bảo vệ thông tin cá nhân trên không gian mạng. Khoản 1 Điều 17 quy định trách nhiệm chung của tổ chức, cá nhân xử lý dữ

liệu cá nhân, tương tự nội dung Luật CNTT nhưng nhấn mạnh hơn đến quy trình thu thập và chia sẻ. Cụ thể:

- **Khoản 1(a)** yêu cầu thu thập thông tin cá nhân phải có sự đồng ý của chủ thể thông tin và phải thông báo rõ phạm vi, mục đích sử dụng.
- **Khoản 1(b)** chỉ cho phép sử dụng thông tin đúng mục đích ban đầu; mọi mục đích mới phải được chủ thể thông tin đồng ý.
- **Khoản 1(c)** nghiêm cấm việc **"cung cấp, chia sẻ, phát tán thông tin cá nhân đã thu thập... cho bên thứ ba"** nếu không có sự đồng ý của chủ thể. Việc website bán dữ liệu cho các nhà quảng cáo là hành vi cung cấp thông tin cá nhân cho bên thứ ba mà không có sự đồng ý, vi phạm trực tiếp quy định này.

Tóm lại, trong tình huống trên, website đã không thực hiện thông báo mục đích (vi phạm Điều 21 Luật CNTT và Điều 17 Luật An toàn thông tin mạng) và đã sử dụng/chia sẻ thông tin ngoài mục đích ban đầu (vi phạm Điều 21.2(b) Luật CNTT và Điều 17.1(c) Luật An toàn thông tin mạng).

Tình hình chung và giải pháp

Thực tế ở Việt Nam cho thấy việc lộ lọt, mua bán thông tin cá nhân đang rất phổ biến. Theo thống kê, khoảng giữa năm 2018 có **427.446 tài khoản Facebook của người Việt Nam bị lộ thông tin cá nhân**, xếp thứ 9 thế giới về mức độ rò rỉ thông tin từ Facebook. Nhiều ứng dụng, dịch vụ trực tuyến (ví dụ: ngân hàng điện tử, dịch vụ y tế trực tuyến, mua bán vé, mạng viễn thông...) cũng yêu cầu người dùng cung cấp thông tin cá nhân, tăng nguy cơ bị lộ lọt. Ngoài ra, "mua bán thông tin cá nhân trái phép" đã được nêu đích danh là một hành vi vi phạm pháp luật trong lĩnh vực công nghệ thông tin. Các vụ việc này cho thấy ý thức bảo vệ dữ liệu của một số doanh nghiệp còn kém, đồng thời việc xử lý vi phạm chưa đủ nghiêm để răn đe.

Giải pháp: Để giảm thiểu vi phạm, cần đồng bộ các biện pháp pháp lý, kỹ thuật và tuyên truyền:

- **Tăng cường thực thi quy định pháp luật:** Các cơ quan quản lý cần kiểm tra, giám sát nghiêm ngặt việc tuân thủ Luật CNTT và Luật An toàn thông tin mạng. Mọi tổ chức thu thập thông tin cá nhân phải minh bạch về mục đích và thủ tục thu thập theo đúng Điều 21 Luật CNTT. Việc xử phạt nghiêm các hành vi vi phạm (như bán thông tin cá nhân trái phép) sẽ nâng cao tính răn đe.
- **Yêu cầu công bố biện pháp bảo vệ thông tin:** Luật An toàn thông tin mạng buộc tổ chức phải "xây dựng và công bố biện pháp xử lý, bảo vệ thông tin cá nhân" của mình. Bắt buộc các website công bố chính sách bảo mật (trong đó nêu rõ cách thức bảo vệ dữ liệu người dùng và cam kết không chia sẻ bên thứ ba trái phép) sẽ giúp người dùng biết quyền lợi và nhà cung cấp chịu trách nhiệm rõ ràng.
- **Tăng cường biện pháp kỹ thuật:** Theo Điều 21.2(c) Luật CNTT, tổ chức phải áp dụng biện pháp quản lý, kỹ thuật để bảo vệ dữ liệu. Các đơn vị cung cấp dịch vụ cần sử dụng

hệ thống mã hóa, tường lửa, phân quyền truy cập và quy trình kiểm tra chặt chẽ nhằm tránh rò rỉ, mất mát dữ liệu cá nhân.

- **Nâng cao ý thức của người dân:** Cần tuyên truyền cho người dùng tự bảo vệ thông tin cá nhân của mình và cẩn trọng khi cung cấp dữ liệu cho các website, ứng dụng. Người dân nên kiểm tra chính sách bảo mật của trang web, chỉ cung cấp thông tin khi thật sự cần thiết và được đảm bảo an toàn.

Kết hợp các giải pháp trên sẽ giúp giảm thiểu tình trạng lạm dụng thông tin cá nhân, bảo vệ tốt hơn quyền riêng tư của người dùng như quy định của Luật Công nghệ thông tin và Luật An toàn thông tin mạng.

Tình huống 6: A là tác giả hai bài báo phân tích về tính " thanh thanh tục tục" trong thơ Hồ Xuân Hương được đăng trên Tạp chí Văn Nghệ số ngày 03/06/2015 và ngày 03/08/2015. B là tác giả cuốn sách " Bình luận Thơ Hồ Xuân Hương" xuất bản ngày 20/11/2017. Trong cuốn sách của mình, B đã tự ý trích dẫn nguyên văn hai bài báo của A, có đề tên tác giả và nguồn gốc tác phẩm rõ ràng, sau đó phân tích và chỉ ra 20 điểm không hợp lý của A khi phân tích về thơ Hồ Xuân Hương. A cho rằng B có hành vi xâm phạm quyền tác giả của mình khi sử dụng tác phẩm mà không xin phép, không trả tiền cho A. Tuy nhiên, B cho rằng ông trính dẫn hợp lý tác phẩm nên không cần xin phép và trả tiền cho A."

(1) Hành vi của A có vi phạm pháp luật không? Nếu có, B đã vi phạm điều khoản nào của luật nào?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự nhóm trên ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

Phân tích vi phạm quyền tác giả

1. Tác phẩm được bảo hộ theo Luật SHTT – Hành vi xâm phạm quyền tác giả của B: Theo Điều 14 Luật Sở hữu trí tuệ, "Tác phẩm văn học, nghệ thuật và khoa học được bảo hộ bao gồm... c) Tác phẩm báo chí". Hai bài báo của A đăng trên Tạp chí Văn nghệ rõ ràng thuộc loại "tác phẩm báo chí" được Luật bảo hộ. Do đó, việc sử dụng nguyên văn toàn bộ nội dung hai bài báo của A để đăng trong sách của B mà không xin phép tác giả là hành vi sử dụng tác phẩm được bảo hộ mà không có quyền. Điều 28 khoản 3 Luật SHTT quy định các hành vi xâm phạm quyền tác giả, trong đó có **"Công bố, phân phối tác phẩm mà không được phép của tác giả"**. Hành vi của B (tự ý công bố/phân phối nguyên văn hai bài báo của A trong sách) trùng với nội dung quy định này. Mặc dù B đã ghi rõ nguồn, tên tác giả, nhưng việc "trích nguyên văn" toàn bộ tác phẩm vượt quá giới hạn cho phép của việc trích dẫn thông thường. Vì vậy, B đã vi phạm Điều 28 Luật SHTT (sửa đổi bổ sung năm 2009, 2019), vi phạm quyền nhân thân và quyền tài sản của tác giả A (cụ thể là quyền cho phép công bố và phân phối tác phẩm).

2. Nội dung điều khoản luật liên quan: Điều 14 Luật SHTT khẳng định "Tác phẩm văn học... bao gồm... tác phẩm báo chí", đồng nghĩa mọi bài báo, bài phân tích trên báo chí đều được bảo hộ quyền

tác giả. Điều 28 Luật SHTT qui định rõ: **"Hành vi xâm phạm quyền tác giả gồm... (3) Công bố, phân phối tác phẩm mà không được phép của tác giả"**. Theo đó, bất kỳ ai muốn công bố, ấn hành hoặc phân phối tác phẩm (hoặc một phần tác phẩm) thuộc quyền tác giả mà chưa được tác giả đồng ý đều là hành vi xâm phạm. Trong tình huống này, B đã đưa nguyên văn bài báo của A vào cuốn sách mà không có sự cho phép của A. Dù B đã ghi nguồn và tác giả, nhưng Luật SHTT không miễn trừ cho việc sao chép toàn bộ nội dung. Theo quy định, trích dẫn có giới hạn phải phục vụ mục đích khoa học, bình luận hoặc phê bình; việc trích dẫn chiếm tỷ lệ lớn (toàn bộ hai bài báo) vẫn phải được phép. Như vậy, hành vi của B vi phạm điều khoản **Điều 28, khoản 3 Luật Sở hữu trí tuệ**.

3. Tình hình vi phạm và giải pháp: Thực trạng xâm phạm quyền tác giả ở Việt Nam hiện còn nghiêm trọng. Tài liệu cho thấy "hiện nay, tình trạng vi phạm SHTT ở nước ta vẫn đang ở mức báo động" và với công nghệ hiện đại "việc sao chép, quảng bá nội dung... ngày càng trở nên dễ dàng, tồn tại sự vi phạm lớn... trong lĩnh vực phần mềm hay bản quyền trong văn học nghệ thuật". Bên cạnh đó, nghiên cứu của liên minh BSA (2018) cho thấy năm 2015 Việt Nam có 78% phần mềm máy tính không bản quyền, phản ánh tâm lý coi nhẹ việc tuân thủ bản quyền. Trong văn học – nghệ thuật, nhiều tác phẩm bị sao chép không phép, tác giả chưa được trả tiền nhuận bút xứng đáng.

Để khắc phục, cần đồng bộ các giải pháp: (a) **Tăng cường công tác giáo dục, nâng cao nhận thức** về tôn trọng quyền tác giả, khuyến khích mua phần mềm, sách báo từ nguồn hợp pháp. Theo khuyến cáo của BSA, tổ chức, cá nhân nên "mua phần mềm từ các nguồn hợp pháp" và thiết lập cơ chế quản lý tài sản phần mềm nội bộ để giảm thiểu vi phạm (tương tự, nên có chính sách khuyến khích mua sách bản quyền, trả nhuận bút cho tác giả). (b) **Thực thi pháp luật nghiêm khắc hơn:** Nhà nước cần xử lý kiên quyết các vụ xâm phạm bản quyền, bao gồm cả truy cứu trách nhiệm hành chính hoặc hình sự đối với hành vi sao chép nguyên văn tác phẩm mà không xin phép. Các ví dụ thực tiễn (ví dụ: vụ phát tán trái phép phim lên mạng xã hội) đã được đưa vào nghị định và luật hình sự về tội xâm phạm bản quyền. (c) **Cập nhật, hoàn thiện khung pháp lý:** Cần bổ sung quy định rõ ràng hơn về giới hạn cho phép của việc trích dẫn trong nghiên cứu, phê bình (như các khoản "sử dụng hợp lý" tương tự quyền tác giả ở nhiều nước) để tránh tranh cãi. Đồng thời, tổ chức hội thảo, tập huấn để phổ biến rộng rãi luật SHTT.

Tóm lại, hành vi của B đã xâm phạm quyền tác giả của A theo Điều 28 Luật SHTT. Để hạn chế vi phạm tương tự, ngoài việc áp dụng nghiêm khắc luật hiện hành, cần nâng cao ý thức tôn trọng bản quyền và tạo cơ chế quản lý, xử lý hiệu quả các vi phạm.

Tình huống 7: A và B là hai bạn rất thân từ khi còn là học sinh tiểu học đến trung học cơ sở, nhưng đến năm lớp 8 thì A và B không còn thân thiết và chơi với nhau nữa. B đã dùng tài khoản mạng xã hội Facebook để đăng tải các thông tin về bí mật của cá nhân A như tính cách, những đặc điểm trên cơ thể, về gia đình A, nói xấu A...và chia sẻ thông tin này đến bạn bè của A và nhận được nhiều bình luận từ người dùng Facebook. A rất buồn và đã đề nghị B gở bỏ các thông tin nhưng B không gỡ dẫn đến A phải bỏ học.

(1) Việc B dùng mạng xã hội Facebook để đăng tải các thông tin về bí mật của cá nhân A như tính cách, những đặc điểm trên cơ thể, về gia đình A có đúng pháp luật không? Nếu có, hãy cho biết vi

phạm điều khoản nào của Luật nào? Những người bạn của A sẽ bị xử lý như thế nào theo điều khoản nào trong luật nào?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự trên ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

Tính pháp lý của hành vi của B và xử lý pháp lý đối với bạn bè của A

Việc B đăng tải công khai các thông tin riêng tư của A (tính cách, đặc điểm cơ thể, về gia đình...) và nói xấu A trên Facebook là **vi phạm pháp luật**. Cụ thể, theo **Luật An ninh mạng 2018**, điều khoản nghiêm cấm "đưa lên không gian mạng những thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật". Việc B tiết lộ các "bí mật cá nhân" của A chính là thực hiện hành vi bị cấm này. Ngoài ra, theo **Luật Công nghệ thông tin 2006**, Điều 21 quy định khi thu thập, xử lý hoặc sử dụng thông tin cá nhân của người khác phải được sự đồng ý của người đó. B không có sự đồng ý của A mà vẫn công khai thông tin cá nhân của A, nên hành vi này cũng vi phạm quy định về bảo vệ dữ liệu cá nhân.

Về phần những người bạn của A (những người xem, bình luận về thông tin do B đăng), nếu họ chỉ đọc hoặc chia sẻ lại (forward) nội dung mà không tự ý chỉnh sửa thì theo luật họ **không bị truy cứu trách nhiệm** về nội dung thông tin đó. Căn cứ Khoản 4 Điều 16 Luật Công nghệ thông tin 2006, "Tổ chức, cá nhân truyền đưa thông tin số của tổ chức, cá nhân khác không phải chịu trách nhiệm về nội dung thông tin đó, trừ trường hợp... lựa chọn và sửa đổi nội dung thông tin được truyền đưa". Nói cách khác, bạn bè của A nếu chỉ bấm "chia sẻ" hoặc bình luận dựa trên nội dung nguyên bản do B đăng và không tự ý thay đổi thì họ không vi phạm luật. Tuy nhiên, nếu họ tự ý chỉnh sửa, thêm thắt hay đăng tải lại nội dung riêng tư này (ví dụ tự chụp ảnh màn hình rồi đăng tiếp), thì hành vi đó cũng có thể bị xem là "đưa lên không gian mạng thông tin bí mật cá nhân" và bị xử lý như B.

Phân tích chi tiết nội dung điều khoản luật liên quan

Điều khoản chính điều chỉnh hành vi trên là **Điều 8 Luật An ninh mạng 2018** (Các hành vi bị nghiêm cấm về an ninh mạng). Trong đó, Luật An ninh mạng quy định rõ: **cấm mọi tổ chức, cá nhân "đưa lên không gian mạng những thông tin thuộc bí mật cá nhân, bí mật gia đình và đời sống riêng tư trái quy định của pháp luật"**. "Bí mật cá nhân" được hiểu là những thông tin riêng tư của một người mà họ không muốn công khai; ví dụ như tình hình sức khỏe, sở thích cá nhân, đặc điểm cơ thể,... "Bí mật gia đình" là thông tin riêng tư của tập thể gia đình như mâu thuẫn gia đình, hoàn cảnh kinh tế, v.v. Khi B đăng thông tin về tính cách, đặc điểm cơ thể hay gia đình A lên Facebook, B đã công khai những thông tin thuộc nhóm này mà không được phép của A – điều luật trên cấm tuyệt đối.

Phân tích sâu hơn, Luật An ninh mạng chia nhỏ các hành vi bị cấm. Ví dụ, **Điều 17 Luật An ninh mạng 2018** liệt kê các hành vi "gián điệp mạng", trong đó có mục nêu rõ nếu cố ý làm lộ thông tin thuộc bí mật cá nhân hay bí mật gia đình **mà gây ảnh hưởng đến danh dự, uy tín, nhân phẩm... của cá nhân khác** thì là hành vi trái pháp luật. Hành vi của B thỏa mãn cả hai yếu tố này: B công khai bí mật cá nhân của A và hành vi đó làm A bị tổn thương (A phải bỏ học vì buồn). Ngoài ra, Điều 21

Luật Công nghệ thông tin 2006 nêu rõ khi thu thập và sử dụng thông tin cá nhân người khác, tổ chức, cá nhân phải có trách nhiệm thông báo cho người đó biết mục đích, phạm vi và được sự đồng ý của họ. B không xin phép A mà vẫn đăng tải thông tin cá nhân của A, tức là đã vi phạm quy định này. Tóm lại, các điều khoản luật trên tập trung bảo vệ **quyền riêng tư, danh dự và lợi ích hợp pháp của cá nhân** trên mạng. Bằng việc đăng nội dung riêng tư của A, B đã trực tiếp xâm phạm những quyền đó, do vậy bị coi là vi phạm Luật An ninh mạng và Luật Công nghệ thông tin.

Tình hình chung và giải pháp đề xuất

Trên thực tế, hiện tượng rò rỉ và lạm dụng thông tin cá nhân trên mạng xã hội xảy ra rất phổ biến ở Việt Nam. Thống kê cho thấy chỉ riêng Facebook đã có **427.446 tài khoản cá nhân tại Việt Nam từng bị lộ thông tin** (dữ liệu cá nhân) – Việt Nam đứng thứ 9 thế giới về mức độ rò rỉ từ Facebook (thống kê tháng 4/2018). Nguyên nhân chủ yếu là người dùng vô tình cung cấp thông tin cá nhân cho các ứng dụng, trò chơi lan truyền trên mạng xã hội, hoặc tiết lộ thông tin riêng tư của nhau trên mạng. Những vụ việc như B đăng thông tin bí mật của A không phải là hiếm: nhiều thanh thiếu niên ở Việt Nam đã từng là nạn nhân của việc lan truyền bậy bạ, bêu xấu trên mạng xã hội, gây hậu quả tâm lý nghiêm trọng.

Để hạn chế các vi phạm kiểu này, cần thực hiện đồng bộ nhiều giải pháp:

- **Tăng cường thực thi pháp luật và xử lý nghiêm:** Các cơ quan chức năng phải kiên quyết xử lý các hành vi đăng tải thông tin riêng tư trái phép. Luật An ninh mạng đã quy định doanh nghiệp cung cấp dịch vụ mạng xã hội phải **xóa bỏ nội dung vi phạm chậm nhất 24 giờ** sau khi nhận được yêu cầu của cơ quan chức năng. Thực thi nghiêm quy định này sẽ giúp hạn chế việc lan truyền thông tin xấu. Ngoài ra, các tổ chức, cá nhân vi phạm có thể bị xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự (về tội xâm phạm bí mật cá nhân, làm nhục người khác) tùy mức độ.
- **Yêu cầu trách nhiệm của nền tảng và doanh nghiệp:** Các mạng xã hội, dịch vụ trực tuyến cần phải tăng cường bảo vệ dữ liệu người dùng. Theo quy định, doanh nghiệp phải **xác thực thông tin người dùng khi đăng ký** tài khoản số và bảo mật thông tin người dùng. Nếu họ phát hiện người dùng đăng tải thông tin cá nhân của người khác trái phép, họ phải chặn và gỡ bỏ ngay. Thực hiện tốt biện pháp này sẽ làm giảm cơ hội tin xấu lan rộng.
- **Giáo dục, tuyên truyền nâng cao nhận thức:** Cần đẩy mạnh tuyên truyền cho mọi người, đặc biệt là học sinh, phụ huynh và giáo viên, về quyền riêng tư trên mạng và những nguy cơ khi chia sẻ thông tin cá nhân. Luật An ninh mạng cũng nhấn mạnh quyền được bảo vệ bí mật cá nhân của trẻ em trên không gian mạng. Nhà trường, gia đình và cộng đồng nên tổ chức các buổi phổ biến kiến thức về an toàn thông tin và quyền trên mạng cho học sinh. Khi ý thức người dùng được nâng cao, họ sẽ thận trọng hơn trong việc chia sẻ hình ảnh, câu chuyện cá nhân và biết cách tố cáo hành vi vi phạm.

- **Giải pháp kỹ thuật:** Người dùng cần sử dụng các công cụ bảo mật (như cài đặt riêng tư trên mạng xã hội, phần mềm diệt virus, không tham gia các trò chơi yêu cầu cung cấp quá nhiều thông tin cá nhân). Bộ Thông tin và Truyền thông có thể tiếp tục phối hợp với các nền tảng mạng xã hội để rà soát, phát hiện và xóa những nội dung xâm hại thông tin cá nhân.

Tóm lại, hành vi đăng tải thông tin riêng tư của người khác trên mạng xã hội là vi phạm nghiêm trọng quy định về an ninh, an toàn thông tin và quyền riêng tư cá nhân. Cần có cả biện pháp pháp lý kiên quyết và giải pháp xã hội – kỹ thuật đồng bộ để ngăn chặn và hạn chế các vi phạm tương tự, bảo vệ quyền của người dùng mạng.

Tình huống 8: Công ty B đã đăng ký bảo hộ kiểu dáng công nghiệp và nhãn hiệu tại Cục sở hữu trí tuệ Việt Nam cho sản phẩm X đang được bán trên thị trường. Nhưng hiện nay trên mạng đã có loại sản phẩm tương tự từ mẫu mã, đến tên nhãn hiệu được bán bởi một công ty khác ở nước ngoài.

(1) Nếu một công ty C nhập sản phẩm tương tự với sản phẩm X từ công ty nước ngoài về tiêu thụ trong nước, công ty C có vi phạm Luật sở hữu trí tuệ không? Nếu có, hãy cho biết vi phạm điều khoản nào của Luật sở hữu trí tuệ? Công ty C sẽ bị xử lý như thế nào theo điều khoản nào trong luật?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự nhóm trên ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

Phân tích vi phạm và quy định pháp luật áp dụng

(1) Hành vi vi phạm Luật SHTT: Theo Điều 3 Luật Sở hữu trí tuệ 2005, đối tượng quyền sở hữu công nghiệp bao gồm cả **kiểu dáng công nghiệp** và **nhãn hiệu** được đăng ký. Doanh nghiệp B đã đăng ký bảo hộ kiểu dáng và nhãn hiệu cho sản phẩm X, nên **công ty C khi nhập khẩu** và kinh doanh sản phẩm có mẫu mã và nhãn hiệu trùng hoặc tương tự sản phẩm X là *xâm phạm* quyền sở hữu công nghiệp của B. Cụ thể:

- *Vi phạm nhãn hiệu:* Công ty C sử dụng dấu hiệu trùng (hoặc tương tự gây nhầm lẫn) với nhãn hiệu đã được bảo hộ cho sản phẩm X để đưa hàng hóa vào thị trường Việt Nam. Theo Khoản 1 Điều 129 Luật SHTT 2005, "sử dụng dấu hiệu trùng với nhãn hiệu được bảo hộ cho hàng hoá, dịch vụ trùng ... mà không được phép của chủ sở hữu nhãn hiệu thì bị coi là xâm phạm quyền đối với nhãn hiệu"thuvienphapluat.vn. Trường hợp sử dụng nhãn hiệu trùng/khá giống trên sản phẩm tương tự, nếu gây nhầm lẫn về nguồn gốc hàng hóa thì đã vi phạm quy định này.

- *Vi phạm kiểu dáng:* Công ty C cũng sử dụng **kiểu dáng công nghiệp** đã được B đăng ký bảo hộ cho sản phẩm X (có thể là bản sao gần như không đổi khác). Điều 126 Luật SHTT 2005 quy định: "Sử dụng kiểu dáng công nghiệp được bảo hộ hoặc kiểu dáng không khác biệt đáng kể với kiểu dáng đó trong thời hạn hiệu lực của văn bằng bảo hộ mà không được phép của chủ sở hữu" cũng là hành vi xâm phạm quyền kiểu dáng công

nghiệplawkey.vn. Như vậy, nhập khẩu sản phẩm y hệt về mẫu mã của X mà không có sự cho phép của B là vi phạm quy định này.

Xử lý theo pháp luật: Hành vi nêu trên có thể bị xử lý theo nhiều biện pháp. Căn cứ Điều 199 Luật SHTT 2005, tổ chức, cá nhân xâm phạm quyền SHTT "tùy theo tính chất, mức độ xâm phạm" có thể bị xử lý bằng biện pháp dân sự, hành chính hoặc hình sựthuvienphapluat.vn. Nói chung, công ty C có thể bị yêu cầu chấm dứt hành vi vi phạm, bồi thường thiệt hại theo quy định của pháp luật, đồng thời có thể bị cơ quan quản lý xử phạt hành chính (ví dụ tiền phạt, tịch thu hàng hóa giả mạo) hoặc bị truy cứu trách nhiệm hình sự nếu cấu thành tội danh "Xâm phạm quyền sở hữu công nghiệp" theo Bộ luật Hình sự (Điều 226 BLHS 2015).

2. Nội dung các điều khoản pháp luật liên quan

- **Điều 126 Luật SHTT 2005 (xâm phạm kiểu dáng công nghiệp):** Quy định các hành vi bị coi là xâm phạm quyền kiểu dáng công nghiệp. Theo đó, việc *"sử dụng kiểu dáng công nghiệp được bảo hộ... mà không được phép của chủ sở hữu"* là hành vi xâm phạmlawkey.vn. Trong tình huống này, kiểu dáng sản phẩm X được B bảo hộ thì mọi sao chép hoặc bắt chước kiểu dáng này bởi C đều vi phạm.
- **Điều 129 Luật SHTT 2005 (xâm phạm nhãn hiệu):** Liệt kê 04 hành vi xâm phạm nhãn hiệu. Trong đó, đáng chú ý có quy định: *"sử dụng dấu hiệu trùng với nhãn hiệu được bảo hộ cho hàng hoá, dịch vụ trùng ... nếu việc sử dụng có khả năng gây nhầm lẫn về nguồn gốc"*thuvienphapluat.vn. Công ty C đã dùng nhãn hiệu giống hệt hoặc tương tự tên nhãn hiệu của B cho hàng hóa tương tự, rõ ràng thuộc trường hợp này. Hành vi này bị coi là xâm phạm quyền nhãn hiệu và bị cấm theo luật.
- **Điều 199 Luật SHTT 2005 (xử lý vi phạm):** Điều khoản này quy định biện pháp xử lý chung đối với hành vi xâm phạm SHTT: *"có thể bị xử lý bằng biện pháp dân sự, hành chính hoặc hình sự"* tùy theo mức độthuvienphapluat.vn. Như vậy, tùy thuộc vào quy mô và hậu quả (giá trị hàng hóa, mức độ thu lợi bất chính...), công ty C có thể bị xử lý tại tòa dân sự (bồi thường, tiêu hủy hàng vi phạm), bị phạt hành chính (theo các Nghị định quy định xử lý vi phạm sở hữu công nghiệp), hoặc thậm chí bị truy cứu hình sự theo Điều 226 BLHS.

(Có thể bổ sung các điều luật khác nếu cần, ví dụ: Điều 202 Luật SHTT 2005 về biện pháp dân sự như buộc chấm dứt hành vi, bồi thường thiệt hại, tiêu hủy hàng hóa giả mạo; Điều 211 Luật SHTT 2005 về xử phạt hành chính xâm phạm SHTT... nhưng các điều này không nằm trong tài liệu đã cho).

3. Thực trạng vi phạm SHTT và giải pháp

Hiện nay, tình trạng xâm phạm sở hữu trí tuệ tại Việt Nam được đánh giá **vẫn ở mức báo động**. Điều này được phản ánh rõ qua tỷ lệ vi phạm bản quyền phần mềm rất cao – khoảng 78% tại Việt Nam năm 2015 (so với 39% trung bình thế giới). Mặc dù dữ liệu này liên quan đến phần mềm, nhưng nó cho thấy chung mức độ lạm dụng tài sản trí tuệ nói chung ở nước ta, bao gồm cả việc sản xuất và

buôn bán hàng nhái, hàng giả về kiểu dáng và nhãn hiệu. Các hình thức vi phạm trong sản xuất – kinh doanh vẫn rất phổ biến do khâu kiểm soát còn lỏng lẻo.

Giải pháp hạn chế vi phạm:

- *Tăng cường thực thi pháp luật:* Cơ quan chức năng (Cục SHTT, Chi cục Quản lý thị trường, hải quan...) cần giám sát và xử lý nghiêm vi phạm xâm phạm kiểu dáng, nhãn hiệu, đặc biệt tại khâu nhập khẩu. Hành vi vi phạm phải bị xử phạt nghiêm minh theo Điều 199 Luật SHTT, cùng các chế tài hành chính (phạt tiền, tiêu hủy hàng hóa vi phạm) hoặc hình sự nếu đủ điều kiện. Ví dụ, theo Điều 226 BLHS, nếu công ty C cố ý nhập hàng giả nhãn hiệu có quy mô lớn thì có thể phải chịu án phạt tù. Đồng thời, cần tăng mức bồi thường thiệt hại trong dân sự để tạo sức răn đe.

- *Kiểm soát thị trường và nâng cao nhận thức:* Đẩy mạnh kiểm tra tại các cửa khẩu, kiểm tra hậu kiểm đối với các lô hàng nhập khẩu, cũng như siết chặt kiểm tra trong sản xuất, lưu thông. Các cơ quan chức năng nên phối hợp với doanh nghiệp sở hữu nhãn hiệu để kịp thời phát hiện và ngăn chặn hàng giả, hàng nhái. Song song đó, tăng cường tuyên truyền nâng cao ý thức tuân thủ SHTT cho cộng đồng doanh nghiệp và người tiêu dùng. Theo khảo sát của BSA năm 2018, doanh nghiệp Việt Nam được khuyến cáo nên "mua phần mềm từ các nguồn hợp pháp" để giảm thiểu rủi ro bản quyền và an ninh mạng. Tương tự, người tiêu dùng và doanh nghiệp nên ưu tiên sử dụng hàng hoá, sản phẩm công nghệ có nguồn gốc rõ ràng, đăng ký nhãn hiệu hợp pháp, nhằm hạn chế thị trường cho hàng nhái.

- *Hoàn thiện pháp luật và hợp tác quốc tế:* Cần cập nhật quy định xử phạt thật rõ ràng, kịp thời khuyến nghị các văn bản hướng dẫn liên quan. Đồng thời, do sản phẩm vi phạm có thể sản xuất ở nước ngoài rồi nhập khẩu, việc hợp tác xuyên biên giới với cơ quan SHTT nước ngoài và thực hiện các điều ước quốc tế về bảo hộ SHTT cũng rất quan trọng để bảo vệ quyền lợi chủ sở hữu trong nước.

Vi phạm sở hữu trí tuệ tại Việt Nam còn diễn biến phức tạp, nhưng bằng các biện pháp quyết liệt nói trên cùng việc tuân thủ quy định Luật SHTT (như Điều 126, 129 và các điều xử lýthuvienphapluat.vnlawkey.vnthuvienphapluat.vn), có thể hạn chế đáng kể các hành vi xâm phạm như trường hợp của công ty C.

Tình huống 9: Do thiếu tiền ăn chơi, A và B đã lập ra nhiều tài khoản facebook ảo để bán điện thoại qua mạng. Hai bạn chụp ảnh những chiếc điện thoại và lấy những hình ảnh trên mạng để đăng bán với giá rẻ hơn so với giá thị trường và đặt ra quy định là khách hàng mua hàng được quyền đổi trả nhưng không được xem hàng trước khi thanh toán tiền. Đến lúc giao hàng, 2 bạn đã bỏ một hộp khẩu trang y tế thay vì điện thoại. Sau đó, 02 bạn xóa tài khoản facebook với mục đích khách hàng sau khi phát hiện sẽ không liên lạc được.

(1) Hãy cho biết hành vi của A và B có vi phạm pháp luật không? Nếu có, hãy cho biết A và B đã vi phạm điều nào, khoản nào của bộ luật nào và sẽ bị xử lý như thế nào?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Giả sử bạn là nhân viên làm việc trong một doanh nghiệp, bạn hãy đưa ra và **giải thích ít nhất 3 lý do** tại sao bạn cần nắm rõ các một số điều khoản của bộ luật mà bạn đã đưa ra ở câu 1.

Hành vi của A và B vi phạm pháp luật?

Hành vi của A và B rõ ràng là gian dối nhằm chiếm đoạt tài sản của người khác. Họ tạo các tài khoản Facebook ảo, đăng tin bán điện thoại với giá rất rẻ để dụ khách; cam kết được đổi trả nhưng không cho xem hàng, rồi giao khẩu trang thay vì điện thoại. Thực chất đây là **thủ đoạn gian dối** để chiếm đoạt tiền của khách hàng, xâm phạm quyền sở hữu tài sản của người khác. Theo tài liệu giảng dạy, hiện có nhiều vụ lừa đảo trên mạng với thủ đoạn giả mạo website, thông tin khuyến mại giả để dụ dỗ, rồi chiếm đoạt tài sản. Hành vi của A và B cũng thuộc dạng "gian dối để chiếm đoạt tài sản".

Vì vậy, A và B đã phạm tội "lừa đảo chiếm đoạt tài sản" quy định tại **Điều 174 Bộ luật Hình sự 2015** (sửa đổi, bổ sung 2017)thuvienphapluat.vn. Cụ thể, Điều 174 định nghĩa: *"lừa đảo chiếm đoạt tài sản là người phạm tội có hành vi áp dụng thủ đoạn gian dối để chiếm đoạt tài sản của người khác"*thuvienphapluat.vn. Tùy theo tình tiết và giá trị tài sản mà A, B có thể bị truy cứu theo các khung hình phạt tương ứng. Nếu giá trị tài sản bị chiếm đoạt từ 2 triệu đến dưới 50 triệu đồng (hoặc thấp hơn nhưng có yếu tố định khung) thì bị phạt tù **6 tháng đến 3 năm**thuvienphapluat.vn. Nếu xác định đây là vụ án có tổ chức (vì A và B cùng thực hiện, nhiều tài khoản giả, tính chuyên nghiệp) thì mức hình phạt thuộc khung 2, phạt tù **2 năm đến 7 năm**thuvienphapluat.vn.

Nội dung chi tiết của điều luật

Điều 174 BLHS 2015 quy định rõ các dấu hiệu cấu thành tội "lừa đảo chiếm đoạt tài sản":

- **Chủ thể:** Bất kỳ người từ đủ 16 tuổi trở lên có năng lực chịu trách nhiệm hình sự.
- **Khách thể:** Quyền sở hữu tài sản của người khác (tài sản là tiền, hàng hóa, v.v.).
- **Mặt chủ quan:** Chủ quan là cố ý, người phạm tội nhận thức và mong muốn việc chiếm đoạt tài sản người khác.
- **Mặt khách quan:** Phải có hành vi **gian dối** (đưa thông tin giả, lừa người khác tin là thật để giao tài sản) và hậu quả là chiếm đoạt tài sản trái pháp luật. Ví dụ như A và B đăng tin bán điện thoại (nội dung gian dối) để khách chuyển tiền rồi giao hàng không đúng. Thủ đoạn gian dối có thể qua lời nói, văn bản, hành động...thuvienphapluat.vn. Hành vi gian dối bắt buộc phải có thì mới cấu thành tội này.
- **Giá trị tài sản:** Tài sản chiếm đoạt phải từ 2.000.000 đồng trở lên (trừ trường hợp dưới 2 triệu nhưng có hậu quả nghiêm trọng hay người phạm tội tái phạm, từng bị xử phạt hành chính vì chiếm đoạt...)thuvienphapluat.vn. Trong tình huống, nếu mỗi chiếc điện thoại giá trên 2 triệu thì giá trị tài sản phù hợp.
- **Hình phạt:** Điều 174 có **bốn khung hình phạt** tùy theo mức độ và tình tiết phạm tội:

- *Khung 1 (Điều 174 khoản 1):* Nếu chiếm đoạt tài sản 2 triệu – dưới 50 triệu đồng (hoặc dưới 2 triệu nhưng có tình tiết tăng nặng như đã bị xử phạt mà còn phạm) thì bị cải tạo không giam giữ đến 3 năm hoặc phạt tù **6 tháng đến 3 năm**thuvienphapluat.vn.
- *Khung 2 (khoản 2):* Nếu phạm tội có tổ chức, có tính chuyên nghiệp, hoặc chiếm đoạt 50 triệu – dưới 200 triệu đồng, hoặc tái phạm nguy hiểm, lợi dụng chức vụ/danh nghĩa, dùng thủ đoạn xảo quyệt… thì bị phạt tù **2 năm đến 7 năm**thuvienphapluat.vn. Trong vụ của A và B, có dấu hiệu "có tổ chức" (cả hai thực hiện cùng kế hoạch lừa đảo), nên có thể áp khung 2.
- *Khung 3 (khoản 3):* Chiếm đoạt 200 – dưới 500 triệu (hoặc lợi dụng thiên tai, dịch bệnh) thì phạt tù **7 đến 15 năm**.
- *Khung 4 (khoản 4):* Chiếm đoạt 500 triệu trở lên (hoặc tình tiết đặc biệt nghiêm trọng) thì phạt tù **12 đến 20 năm**.

Như vậy, A và B sẽ bị truy cứu trách nhiệm hình sự theo Điều 174 BLHS. Cụ thể, nếu tổng giá trị tài sản lừa đảo đủ lớn hoặc có tình tiết tăng nặng (như có tổ chức), họ sẽ bị phạt tù. Ví dụ, theo Khung 1 nếu thu lợi dưới 50 triệu thì mức phạt 6 tháng – 3 năm tùthuvienphapluat.vn; nếu là hành vi có tổ chức thì phạt tù 2 – 7 nămthuvienphapluat.vn. Ngoài hình phạt tù, tùy mức độ sẽ có thêm hình phạt bổ sung (cấm đảm nhiệm chức vụ, cấm hành nghề…).

Lý do nhân viên cần nắm rõ điều luật này

Việc nhân viên (đặc biệt trong lĩnh vực kinh doanh trực tuyến) am hiểu các quy định như Điều 174 BLHS là rất cần thiết. Dưới đây là một số lý do:

- **Bảo vệ quyền lợi hợp pháp của bản thân và doanh nghiệp:** Theo Luật An toàn thông tin mạng, mức độ cá nhân/doanh nghiệp là phải "bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia" hoạt động (ví dụ thương mại điện tử). Nếu nhân viên hiểu luật, họ sẽ biết mình và công ty không được thực hiện hành vi gian lận, đồng thời biết khi nào khách hàng bị lừa để kịp thời bảo vệ quyền lợi (khởi kiện, tố cáo). Nắm luật giúp tránh các rủi ro về quyền sở hữu, hợp đồng, và danh tiếng.
- **Tuân thủ quy định pháp luật trong hoạt động kinh doanh:** Mọi hoạt động kinh doanh, đặc biệt trên mạng, đều phải "đúng quy định của pháp luật". Nếu nhân viên am hiểu luật, công ty sẽ thiết kế quy trình bán hàng và marketing hợp pháp (ví dụ không giấu giá, không ép người mua không được kiểm hàng). Ngược lại, nếu thiếu hiểu biết, có thể vô tình phạm luật, khiến công ty bị xử phạt hành chính hoặc kiện cáo, ảnh hưởng uy tín.
- **Giảm thiểu rủi ro pháp lý và tranh chấp:** Hiểu luật giúp nhân viên chủ động nhận diện những hành vi rủi ro như giả mạo, lừa đảo, quảng cáo sai sự thật… và ngăn chặn chúng. Trong ví dụ, nếu nhân viên biết hành vi đóng giả bán hàng là tội phạm, họ sẽ cảnh báo

hoặc từ chối tham gia. Điều này giúp bảo vệ công ty khỏi việc bị "vạ lây" (nếu khách hàng lầm tưởng ai đó lừa họ), và bản thân nhân viên không bị lôi kéo vào hoạt động phi pháp.

- **Duy trì uy tín và tạo niềm tin với khách hàng:** Khi nhân viên hiểu rõ quy định, họ sẽ biết cách minh bạch thông tin (giá bán, điều kiện đổi trả, thời gian giao hàng...) theo đúng Nghị định về thương mại điện tử (ví dụ Điều 28, 31, 33 NĐ 52/2013/NĐ-CP). Điều này giúp khách hàng tin tưởng và tuân thủ pháp luật, tránh tranh chấp và khiếu nại. Nắm luật cũng giúp xử lý hợp lý khi phát sinh vấn đề (ví dụ biết quyền khiếu nại khi bị lừa).

Tóm lại, nhân viên hiểu biết pháp luật (cụ thể là các quy định về thương mại điện tử và hình sự như Điều 174 BLHS) sẽ bảo vệ được quyền lợi cho chính mình và doanh nghiệp, giúp công ty hoạt động an toàn, tuân thủ quy định, tránh được các hậu quả pháp lý nghiêm trọng.

Tình huống 10: Sinh viên A thực tập tại công ty chuyên cung cấp phần mềm ERP cho doanh nghiệp, sinh viên này được giao nhiệm vụ hỗ trợ một nhân viên chính thức của công ty cùng tham gia bảo trì một hệ thống ERP cho một doanh nghiệp hoạt động trong lĩnh vực sản xuất và cung cấp thiết bị văn phòng. Do vậy, sinh viên A dễ dàng tiếp cận danh sách các công ty cung cấp nguồn nguyên liệu cho doanh nghiệp này. Trong một lần trò chuyện, sinh viên A đã vô tình tiết lộ các công ty cung cấp nguồn nguyên liệu với sinh viên B đang thực tập tại công ty đối thủ.

(1) Vậy sinh viên A đã vi phạm nguyên tắc nào của bộ quy tắc ứng xử ACM?

(2) Trình bày chi tiết nguyên tắc trên?

(3) Giả sử bạn là nhân viên làm việc trong ngành CNTT, bạn hãy **đưa ra và giải thích ít nhất 3 lý do** tại sao bạn cần nắm rõ các một số điều khoản luật trong luật an ninh mạng.

1. Nguyên tắc ACM bị vi phạm

Trong tình huống trên, sinh viên A đã tiết lộ danh sách các nhà cung cấp nguyên liệu – thông tin nội bộ quan trọng của doanh nghiệp – cho người của công ty đối thủ. Theo Bộ quy tắc đạo đức của Hiệp hội máy tính ACM, hành vi này vi phạm **nguyên tắc bảo mật và danh dự** (confidentiality/honor confidentiality). Nguyên tắc này yêu cầu chuyên gia CNTT phải bảo vệ thông tin bí mật được giao và không được tiết lộ cho bên thứ ba khi chưa có sự cho phép hoặc yêu cầu hợp pháp. Hành động tiết lộ thông tin nhà cung cấp của sinh viên A là vi phạm trực tiếp tính bảo mật thông tin của tổ chức khách hàng, tương tự như cấm "tiết lộ bí mật... đã được pháp luật quy định" trong Luật CNTT và cấm "xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác" trong Luật An toàn thông tin mạng.

2. Chi tiết nguyên tắc bảo mật thông tin (ACM)

Nguyên tắc bảo mật trong ACM yêu cầu chuyên gia CNTT "giữ kín các thông tin bảo mật" và chỉ tiết lộ khi được phép. Cụ thể, ACM quy định nếu được giao thông tin thương mại bí mật, chiến lược kinh doanh, dữ liệu khách hàng... thì phải bảo vệ chúng một cách tối đa, chỉ chia sẻ khi có lý do pháp luật. Tương tự, Luật Công nghệ thông tin 2006 (Điều 12.2(c)) nghiêm cấm "tiết lộ bí mật nhà nước, bí mật quân sự, an ninh, kinh tế, đối ngoại và những bí mật khác đã được pháp luật quy định". Điều này bao hàm cả bí mật kinh doanh của doanh nghiệp. Luật An toàn thông tin mạng (ATTTM) cũng quy

định rõ nguyên tắc này: “Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác”. Các quy định pháp luật này khẳng định rằng việc tiết lộ thông tin riêng tư, thông tin nội bộ của tổ chức mà không có sự đồng ý đều là vi phạm pháp luật.

Do đó, nguyên tắc ACM về bảo mật (honor confidentiality) đòi hỏi sinh viên A phải giữ bí mật thông tin đã được giao – tức danh sách nhà cung cấp – và không tiết lộ cho bất kỳ ai (trừ trường hợp được phép). Việc A vô tình tiết lộ thông tin này đã phá vỡ nguyên tắc giữ bí mật thông tin đã giao phó. Luật ATTTM và Luật CNTT cho thấy rõ việc xâm phạm bí mật thông tin của người khác là hành vi bị cấm. Theo đó, sinh viên A không những vi phạm đạo đức nghề nghiệp (bộ quy tắc ACM), mà còn có thể liên đới vi phạm pháp luật về bảo vệ thông tin bí mật của tổ chức khách hàng.

3. Tại sao cần nắm rõ Luật An ninh mạng

Là một nhân viên CNTT, việc hiểu rõ Luật An ninh mạng giúp chúng ta tuân thủ pháp luật và bảo vệ tổ chức lẫn cá nhân trong môi trường số. Cụ thể có thể kể ra ba lý do chính:

- **Bảo vệ quyền lợi hợp pháp của cá nhân và doanh nghiệp:** Luật An ninh mạng và Luật ATTTM 2015 đều nhấn mạnh mục tiêu bảo vệ quyền lợi hợp pháp của các tổ chức, cá nhân tham gia không gian mạng. Ví dụ, Luật ATTTM 2015 nêu rõ “bảo vệ quyền và lợi ích hợp pháp của tổ chức, cá nhân tham gia hoạt động an toàn thông tin mạng”. Tương tự, Luật An ninh mạng 2018 quy định đấu tranh chống các thông tin độc hại, “xâm phạm đến… quyền và lợi ích hợp pháp của các cá nhân, tổ chức” trên mạng. Nắm các điều khoản này giúp chúng ta thực hiện đúng nghĩa vụ bảo vệ dữ liệu cá nhân, thông tin công ty, tránh để lộ dữ liệu nhạy cảm gây thiệt hại cho mình và khách hàng. Nhân viên CNTT am hiểu pháp luật sẽ biết cách tuân thủ quy định, ví dụ chỉ thu thập, xử lý thông tin sau khi có sự đồng ý của người dùng, qua đó bảo vệ tốt hơn quyền riêng tư và lợi ích hợp pháp của mọi bên liên quan.
- **Phòng ngừa, phát hiện và ứng phó với nguy cơ mất an toàn:** Luật An ninh mạng khuyến khích các tổ chức tăng cường giám sát, phòng chống rủi ro an ninh mạng. Thông qua việc nắm luật, nhân viên CNTT hiểu rõ các quy định về biện pháp an ninh, trách nhiệm của doanh nghiệp khi phát hiện hoặc được yêu cầu xử lý thông tin nguy hại. Ví dụ, theo Điều 26 Luật An ninh mạng 2018, khi có yêu cầu của cơ quan chức năng, doanh nghiệp phải ngăn chặn và xóa bỏ thông tin vi phạm trong vòng 24 giờ. Luật cũng yêu cầu các dịch vụ viễn thông, Internet phải có cơ chế báo cáo, hỗ trợ cơ quan điều tra và bảo vệ người dùng. Việc am hiểu những quy định này giúp cán bộ CNTT kịp thời phát hiện và đáp ứng các yêu cầu (như lưu giữ log, xóa thông tin xấu), từ đó ứng phó hiệu quả với các cuộc tấn công mạng và đảm bảo hệ thống luôn an toàn theo luật định.
- **Tuân thủ nghĩa vụ pháp lý, tránh bị xử phạt:** Các doanh nghiệp và cá nhân cung cấp dịch vụ mạng có nhiều nghĩa vụ theo Luật An ninh mạng. Chẳng hạn, Điều 26.3 Luật An ninh mạng 2018 quy định các doanh nghiệp viễn thông, Internet phải lưu trữ dữ liệu cá nhân và dữ liệu quan hệ của người dùng tại Việt Nam. Doanh nghiệp còn phải sẵn sàng cung cấp thông tin người dùng cho cơ quan chức năng khi có yêu cầu. Nếu không nắm rõ

luật, nhân viên CNTT có thể vô tình vi phạm quy định như lưu trữ sai địa điểm dữ liệu hoặc không kịp thời hỗ trợ điều tra, dẫn đến bị xử phạt hành chính hoặc hình sự. Vì vậy, hiểu biết Luật An ninh mạng giúp chúng ta triển khai các biện pháp kỹ thuật phù hợp (mua máy chủ lưu trữ trong nước, thiết lập quy trình cung cấp log cho cơ quan điều tra...) và chủ động tuân thủ, tránh vi phạm pháp luật ngoài ý muốn.

Tóm lại, nắm vững các điều khoản của Luật An ninh mạng là yêu cầu bắt buộc đối với nhân viên CNTT. Nó giúp chúng ta bảo vệ tốt nhất dữ liệu và quyền lợi của bản thân, của doanh nghiệp và khách hàng; đồng thời phòng ngừa và ứng phó hiệu quả với các đe dọa an ninh mạng. Việc tuân thủ Luật không chỉ là trách nhiệm pháp lý mà còn nâng cao uy tín và an toàn cho tổ chức mình.

Tình huống 11: Trưa 13/11/2017, Nguyễn Văn T. mua vé xem phim "Cô Ba Sài Gòn" ở rạp Lottle Cinema Vũng Tàu. T. đã dùng điện thoại quay livestream nội dung phim đang chiếu lên Facebook.

(1) Hãy cho biết hành vi của Nguyễn Văn T. có vi phạm Luật sở hữu trí tuệ không? Nếu có, hãy cho biết Nguyễn Văn T. đã vi phạm điều nào của Luật sở hữu trí tuệ và sẽ bị xử lý như thế nào theo điều nào trong luật?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Giả sử bạn là nhân viên làm việc trong ngành CNTT, bạn hãy **đưa ra và giải thích ít nhất 3 lý do** tại sao bạn cần nắm rõ các một số điều khoản luật trong luật an ninh mạng.

Phân tích tình huống vi phạm Luật Sở hữu trí tuệ và Luật An ninh mạng

Hành vi của Nguyễn Văn T. và Luật sở hữu trí tuệ

Bộ phim "Cô Ba Sài Gòn" là một **tác phẩm điện ảnh** được bảo hộ theo Luật Sở hữu trí tuệ (Luật SHTT). Theo Điều 28 Luật SHTT, các hành vi xâm phạm quyền tác giả bao gồm việc **"Công bố, phân phối tác phẩm mà không được phép của tác giả"**. Hành vi Nguyễn Văn T. dùng điện thoại quay phim đang chiếu và livestream lên Facebook chính là **phát tán công khai nội dung phim** mà không có sự cho phép của chủ sở hữu quyền tác giả, thuộc trường hợp bị cấm nêu trên. Như vậy, T. đã vi phạm Điều 28 khoản 3 Luật SHTT. Hậu quả, theo quy định pháp luật, anh T. có thể bị xử phạt hành chính hoặc bị truy cứu trách nhiệm hình sự tùy mức độ vi phạm, căn cứ vào các điều khoản liên quan của Luật SHTT và các văn bản hướng dẫn thi hành.

Nội dung điều khoản Điều 28 Luật SHTT

Điều 28 Luật SHTT quy định các hành vi xâm phạm quyền tác giả. Cụ thể, khoản 3 ghi rõ: **"Công bố, phân phối tác phẩm mà không được phép của tác giả"**. Cụm từ "công bố, phân phối tác phẩm" bao gồm mọi hành động làm cho tác phẩm (trong trường hợp này là bộ phim) được phổ biến rộng rãi đến công chúng, ví dụ như chiếu phim, phát hành đĩa, hoặc đăng tải trực tuyến. Yếu tố **"không được phép của tác giả"** có nghĩa là người phát tán tác phẩm phải có sự đồng ý của chủ sở hữu bản quyền. Trong tình huống này, anh T. đã trực tiếp công chiếu bộ phim qua Facebook mà không được cấp phép của hãng phim hay tác giả, nên đã phạm vào nội dung bị cấm của Điều 28. Điều luật này khẳng định quyền của tác giả/pháp nhân sở hữu bản quyền được độc quyền công bố và phân phối

tác phẩm. Phân tích chi tiết, quy định tại Điều 28 khoản 3 yêu cầu **"không được phép"** nghĩa là mọi hành vi phát tán tác phẩm phải được chủ sở hữu cho phép; nếu không, đó là hành vi xâm phạm quyền tác giả. Vì vậy, hành động livestream phim của Nguyễn Văn T. vi phạm nguyên tắc này.

Lý do cần nắm Luật An ninh mạng (với nhân viên CNTT)

Nhân viên ngành CNTT cần nắm rõ các quy định của Luật An ninh mạng (trong đó có cả Luật An toàn thông tin mạng 2015 và Luật An ninh mạng 2018) vì các lý do sau:

- **Trách nhiệm bảo đảm an toàn thông tin**: Luật quy định mọi cơ quan, tổ chức và cá nhân đều có trách nhiệm bảo đảm an toàn thông tin mạng. Cụ thể, Điều 4 quy định "Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng" và "Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác". Đối với chuyên viên CNTT, hiểu rõ quy định này giúp thiết kế, quản lý hệ thống đúng pháp luật, đồng thời tránh vô ý vi phạm khi triển khai giải pháp công nghệ.
- **Tuân thủ nghĩa vụ pháp lý của doanh nghiệp**: Luật An ninh mạng 2018 quy định chặt chẽ các nghĩa vụ của doanh nghiệp cung cấp dịch vụ mạng, ví dụ: phải **lưu trữ dữ liệu người dùng tại Việt Nam** (Điều 26.3) và phải **ngừng cung cấp dịch vụ/xóa bỏ thông tin vi phạm** theo yêu cầu của cơ quan chức năng trong vòng 24 giờ. Ngoài ra, doanh nghiệp phải xác thực thông tin người dùng và cung cấp thông tin này cho lực lượng an ninh mạng khi có yêu cầu. Nhân viên CNTT cần biết để thiết lập hệ thống, quy trình xử lý dữ liệu và hỗ trợ nghiệp vụ đúng quy định, tránh để công ty vi phạm luật (ví dụ lưu trữ dữ liệu ra nước ngoài hay không kịp thời cung cấp log người dùng).
- **Bảo vệ người dùng (đặc biệt trẻ em)**: Luật An ninh mạng có chương về **quyền trẻ em trên không gian mạng**. Ví dụ, Điều 29 ghi rằng "Trẻ em có quyền được bảo vệ... khi tham gia trên không gian mạng" và yêu cầu các chủ trang thông tin, nhà cung cấp dịch vụ kiểm soát nội dung để không gây hại đến trẻ em. Nhân viên CNTT cần lưu ý các quy định này khi phát triển, quản lý hệ thống mạng xã hội, diễn đàn, game online... đảm bảo có cơ chế chặn lọc nội dung độc hại, bảo vệ trẻ em; đồng thời cần tuân thủ quy định về quyền riêng tư cá nhân.

Như vậy, việc nắm rõ các điều khoản của Luật An ninh mạng giúp nhân viên CNTT hiểu rõ **trách nhiệm pháp lý, nghĩa vụ và hành vi được/nên làm** trong quản lý an toàn hệ thống thông tin, đồng thời bảo vệ tổ chức và người dùng trước các yêu cầu của pháp luật.

Tình huống 12: Lợi dụng lúc A không có nhà, những người bạn của A đã vào trang facebook cá nhân của A chụp ảnh lại các đoạn tin nhắn có nội dung liên quan những người bạn này. Sau đó, những người bạn của A phát tán lên mạng các đoạn tin nhắn này kèm theo những lời lẽ xúc phạm A.

(1) Những người bạn của A có vi phạm pháp luật không? Nếu có, hãy cho biết vi phạm điều khoản nào của Luật nào? Những người bạn của A sẽ bị xử lý như thế nào theo điều khoản nào trong luật nào?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Giả sử bạn là nhân viên làm việc trong ngành CNTT, bạn hãy **đưa ra và giải thích ít nhất 3 lý do** tại sao bạn cần nắm rõ các một số điều khoản luật trong luật an ninh mạng.

Phân tích tình huống và quy định pháp luật liên quan

(1) Hành vi vi phạm pháp luật

Hành vi của bạn bè A rõ ràng vi phạm quy định của pháp luật về an toàn thông tin. Cụ thể, Luật Công nghệ Thông tin 2006 (Luật CNTT) tại **Điều 72, Khoản 2** nghiêm cấm bất kỳ tổ chức, cá nhân nào *"xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng"* cũng như *"bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng"*. Hành vi lợi dụng lúc A vắng nhà để vào Facebook của A và chụp ảnh các tin nhắn là đã **xâm nhập trái phép** và sử dụng thông tin của người khác, thuộc một trong những hành vi bị cấm nói trên. Ngoài ra, việc phát tán các tin nhắn kèm lời lẽ xúc phạm A cũng vi phạm Luật An ninh mạng 2018. Theo quy định tại **Điều 8** của Luật An ninh mạng 2018, **cấm đăng tải, phát tán thông tin trên không gian mạng có nội dung "làm nhục, vu khống" hoặc "xâm phạm quyền và lợi ích hợp pháp của tổ chức, cá nhân"**. Trong tình huống này, bạn bè của A đã đăng tải thông tin có tính chất làm nhục, bôi nhọ trên mạng, do đó phạm quy định này. Vì vậy, **hành vi của bạn bè A đã vi phạm** Điều 72, Khoản 2 Luật CNTT 2006 và Điều 8 Luật An ninh mạng 2018.

Hành vi vi phạm nêu trên có thể bị **xử lý hình sự hoặc hành chính** tùy mức độ. Về hành chính, Nghị định 15/2020/NĐ-CP quy định xử phạt vi phạm hành chính trong lĩnh vực công nghệ thông tin có thể áp dụng (ví dụ phạt tiền với hành vi xâm nhập, chiếm đoạt thông tin cá nhân). Nếu đủ dấu hiệu cấu thành tội phạm (xâm phạm bí mật cá nhân, gia đình hoặc thư tín, điện thoại, mạng máy tính), người vi phạm có thể bị xử lý hình sự theo Bộ luật Hình sự (tội xâm phạm bí mật đời tư, tội xâm phạm an ninh mạng, v.v.).

(2) Nội dung và phân tích điều khoản luật bị vi phạm

Luật Công nghệ Thông tin 2006, Điều 72 – Bảo đảm an toàn, bí mật thông tin nêu rõ như sau: *"Tổ chức, cá nhân không được thực hiện một trong những hành vi sau: a) Xâm nhập, sửa đổi, xóa bỏ nội dung thông tin của tổ chức, cá nhân khác trên môi trường mạng; ... d) Bẻ khóa, trộm cắp, sử dụng mật khẩu, khóa mật mã và thông tin của tổ chức, cá nhân khác trên môi trường mạng"*. Nội dung này nghĩa là **mọi hành vi truy cập hoặc thay đổi thông tin trên mạng mà không được phép của chủ sở hữu đều bị cấm**. Cụ thể, khoản (a) cấm bất kỳ ai tự ý đột nhập, làm thay đổi hoặc xóa thông tin của người khác trên mạng; khoản (d) cấm việc "bẻ khóa" (giải mã), trộm mật khẩu, sử dụng trái phép khóa mã hoặc chiếm đoạt thông tin của người khác.

Điều khoản này được đặt ra nhằm **bảo vệ tính an toàn và bí mật thông tin trên môi trường mạng**. Bất kỳ hành động xâm nhập trái phép hoặc sử dụng tài khoản, dữ liệu của người khác mà không có sự đồng ý đều có thể làm sai lệch, lộ lọt hoặc mất mát thông tin cá nhân, do đó nguy hiểm cho quyền lợi của người bị hại. Trong trường hợp của A, các bạn của A không có quyền vào Facebook của A nhưng vẫn truy cập và chụp lại tin nhắn cá nhân. Hành vi này thuộc phạm vi bị cấm tại cả mục a)

(xâm nhập và sao chép thông tin người khác) và mục d) (sử dụng mật khẩu, thông tin của người khác).

Về chế tài, Điều 72 là điều khoản chung quy định hành vi bị nghiêm cấm. Khi vi phạm, tùy tính chất nghiêm trọng mà có thể bị **xử phạt vi phạm hành chính** theo Nghị định 15/2020/NĐ-CP (quy định xử phạt trong lĩnh vực công nghệ thông tin) hoặc **truy cứu trách nhiệm hình sự** (nếu gây hậu quả nghiêm trọng, xâm phạm bí mật cá nhân, đời tư). Ngoài ra, việc xúc phạm A qua mạng cũng vi phạm Luật An ninh mạng 2018: theo khoản 1 Điều 8 Luật An ninh mạng, **cấm đăng tải thông tin "làm nhục, vu khống" người khác trên không gian mạng**. Nội dung này một lần nữa khẳng định hành vi phát tán tin nhắn kèm lời lẽ xúc phạm đã là hành vi trái pháp luật.

(3) Ít nhất 3 lý do người làm CNTT cần nắm Luật An ninh mạng

- **Bảo đảm tuân thủ các quy định về dữ liệu và hạ tầng mạng.** Luật An ninh mạng 2018 quy định rõ nhiều nghĩa vụ liên quan đến công nghệ thông tin. Chẳng hạn, Điều 26.3 yêu cầu các doanh nghiệp (trong và ngoài nước) cung cấp dịch vụ viễn thông, Internet, dịch vụ mạng phải **lưu trữ dữ liệu người dùng tại Việt Nam** và đặc biệt đặt văn phòng đại diện tại Việt Nam. Là người làm trong ngành CNTT, bạn phải hiểu yêu cầu này để thiết kế hạ tầng phù hợp (lưu trữ máy chủ trong nước, tuân thủ quy định truy xuất dữ liệu), tránh vi phạm luật khi quản lý thông tin người dùng.
- **Bảo vệ người dùng và ngăn chặn thông tin vi phạm.** Luật buộc các nhà cung cấp dịch vụ mạng phải kiểm soát nội dung và gỡ bỏ thông tin vi phạm nhanh chóng. Cụ thể, nếu người dùng đăng tải hoặc chia sẻ thông tin bị nghiêm cấm, doanh nghiệp phải **ngăn chặn và xóa bỏ thông tin trong vòng 24 giờ** kể từ khi nhận yêu cầu của cơ quan quản lý. Là nhân viên CNTT, bạn cần nắm quy định này để đảm bảo hệ thống của mình có cơ chế giám sát và xử lý đúng hạn, tránh bị phạt do để nội dung trái phép tồn tại.
- **Hợp tác với cơ quan chức năng và bảo vệ an ninh mạng.** Luật An ninh mạng quy định rõ trách nhiệm phối hợp với lực lượng chức năng. Ví dụ, các doanh nghiệp cung cấp dịch vụ mạng phải **xác thực thông tin người dùng khi đăng ký tài khoản, bảo mật tài khoản và cung cấp đầy đủ thông tin của người dùng khi có yêu cầu** từ cơ quan an ninh mạng. Điều này đòi hỏi người làm CNTT hiểu quy trình quản lý tài khoản, lưu nhật ký truy cập và sẵn sàng cung cấp dữ liệu khi được yêu cầu. Ngoài ra, Luật cũng đặt nặng vấn đề bảo vệ trẻ em: Điều 29 quy định chủ quản hệ thống thông tin và doanh nghiệp mạng có trách nhiệm kiểm soát, ngăn chặn thông tin gây hại cho trẻ em. Nắm rõ các quy định này giúp bạn xây dựng chính sách an toàn nội dung và bảo vệ đối tượng dễ bị tổn thương trên môi trường mạng.

Những lý do trên đều xuất phát từ quy định của Luật An ninh mạng 2018 trong việc bảo vệ **tính an toàn, bảo mật của hệ thống thông tin và lợi ích hợp pháp của người dân**. Người làm CNTT nắm vững luật sẽ thiết kế, vận hành hệ thống đúng quy định, tránh vi phạm và đảm bảo môi trường mạng an toàn cho mọi người.

Tình huống 13: Khi ông A đi thăm người thân ở bệnh viện đã chụp hình trong phòng bệnh và đăng trên Facebook. Trong hình mà ông A đã đăng trên Facebook có hình của bà B là bệnh nhân khác trong phòng bệnh. Bà B không muốn người khác biết mình đang nằm viện nên gọi điện thoại yêu cầu ông A không được đưa hình ảnh của mình trên Facebook. Ông A từ chối yêu cầu của bà B vì cho rằng mình có toàn quyền với hình ảnh mà mình đã chụp.

(1) Hành vi của ông A có vi phạm pháp luật không? Nếu có, ông A đã vi phạm điều khoản nào của luật nào? Nếu bà B gởi đơn khiếu nại cho cơ quan có thẩm quyền thì ông A sẽ bị xử phạt tại điều khoản nào của luật nào?

(2) Bạn hãy trình bày và **phân tích chi tiết nội dung của điều khoản luật này**.

(3) Giả sử bạn là nhân viên làm việc trong ngành CNTT, bạn hãy **đưa ra và giải thích ít nhất 3 lý do** tại sao bạn cần nắm rõ các một số điều khoản luật trong luật an ninh mạng.

Câu 1: Hành vi của ông A có vi phạm pháp luật không? Nếu có, vi phạm điều khoản nào của luật nào? Nếu bà B khiếu nại, ông A bị xử phạt theo điều khoản nào của luật nào?

Ông A đã **vi phạm** quy định của Luật về an toàn thông tin mạng. Cụ thể, Luật An toàn thông tin mạng 2015 quy định: *"Thu thập, sử dụng, phát tán, kinh doanh **trái pháp luật** thông tin cá nhân của người khác"* là một hành vi bị nghiêm cấm. Việc ông A chụp hình (thu thập thông tin cá nhân) và đưa lên mạng xã hội mà không có sự đồng ý của bà B đã trực tiếp vi phạm Điều 7, Khoản 5 của Luật này. Do đó, ông A chịu trách nhiệm pháp lý về hành vi xâm phạm thông tin cá nhân của người khác. Nếu bà B khiếu nại, ông A sẽ bị xử phạt theo quy định liên quan trong Luật An toàn thông tin mạng (cụ thể là các quy định áp dụng xử lý vi phạm hành chính trong lĩnh vực công nghệ thông tin), và có thể chịu chế tài theo điều khoản tương ứng trong Luật An ninh mạng 2018 (ví dụ Điều 17, Khoản 1 cấm xâm phạm thông tin cá nhân trên không gian mạng).

Câu 2: Nội dung và phân tích điều khoản vi phạm

Điều 7, Khoản 5 Luật An toàn thông tin mạng 2015 **nêu rõ**: *"Thu thập, sử dụng, phát tán, kinh doanh trái pháp luật thông tin cá nhân của người khác"* là hành vi nghiêm cấm. Điều này có nghĩa là mọi tổ chức, cá nhân đều **không được phép** thu thập hay công bố (phát tán) thông tin cá nhân của người khác nếu không có cơ sở pháp lý. Trong tình huống trên, hình ảnh của bà B chính là thông tin cá nhân đặc biệt (liên quan đến đời tư), việc ông A **đưa hình ảnh bà B lên Facebook mà không được bà B đồng ý là hành vi phát tán thông tin cá nhân trái pháp luật**. Hành vi này bị Luật cấm vì nó xâm phạm quyền riêng tư, danh dự của người khác. Ngoài ra, theo Luật Công nghệ thông tin 2006, Điều 21 cũng quy định: khi thu thập và sử dụng thông tin cá nhân của người khác, cá nhân phải **thông báo cho họ biết mục đích và phạm vi sử dụng**. Ông A đã không thông báo hay xin phép bà B trước khi công bố hình ảnh của bà. Như vậy, căn cứ vào Điều 7, Khoản 5 Luật An toàn thông tin mạng 2015 (và Điều 21 Luật CNTT 2006) thì hành vi của ông A là **trái pháp luật** và phải chịu xử lý theo quy định.

Câu 3: Ba lý do cần nắm rõ một số điều khoản của Luật An ninh mạng

- **Đảm bảo tuân thủ quy định lưu trữ và bảo mật dữ liệu.** Luật An ninh mạng 2018 yêu cầu các doanh nghiệp công nghệ tại Việt Nam phải lưu trữ **dữ liệu quan trọng** trong nước. Ví dụ, *"Dữ liệu về thông tin cá nhân, dữ liệu về mối quan hệ của người sử dụng dịch vụ... do người sử dụng dịch vụ tại Việt Nam tạo ra phải lưu trữ tại Việt Nam"*. Nhân viên CNTT cần biết quy định này để thiết kế hệ thống lưu trữ dữ liệu hợp pháp, tránh rủi ro vi phạm (ví dụ đưa dữ liệu ra nước ngoài trái phép có thể bị xử phạt) và bảo vệ tốt hơn thông tin người dùng.
- **Bảo đảm an toàn thông tin và yêu cầu bảo mật.** Luật này quy định các biện pháp an ninh mạng và các nguyên tắc bảo vệ thông tin trên môi trường mạng. Mục tiêu luật nêu rõ nhằm *"bảo vệ sự an toàn thông tin trên ba phương diện: tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin"*. Nhân viên CNTT cần nắm rõ các quy định này để thiết kế, vận hành hệ thống sao cho đáp ứng các yêu cầu bảo vệ chống mất mát, đánh cắp hay rò rỉ dữ liệu (ví dụ phải áp dụng các biện pháp bảo mật kỹ thuật cần thiết). Việc nắm quy định giúp chủ động phòng ngừa sự cố an ninh, cũng như dễ dàng triển khai các giải pháp mã hóa, tường lửa, hệ thống giám sát mạng phù hợp.
- **Tuân thủ trách nhiệm phối hợp với cơ quan chức năng.** Luật An ninh mạng quy định cụ thể trách nhiệm của doanh nghiệp cung cấp dịch vụ mạng. Ví dụ, Điều 26.3 quy định doanh nghiệp mạng phải *"xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản của người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng... khi có yêu cầu"*. Nhân viên CNTT cần biết để thiết kế tính năng xác thực tài khoản và lưu trữ nhật ký người dùng đúng quy định. Điều này giúp công ty hợp tác với cơ quan chức năng khi điều tra vi phạm trên mạng (ví dụ điều tra hành vi tấn công mạng), đồng thời tránh bị xử phạt vì không cung cấp hoặc bảo vệ thông tin người dùng theo pháp luật.

Tóm lại, am hiểu Luật An ninh mạng giúp nhân viên CNTT triển khai hạ tầng mạng hợp pháp (như lưu trữ dữ liệu đúng nơi, áp dụng biện pháp bảo mật) và chủ động ứng phó với yêu cầu của pháp luật, qua đó bảo vệ tổ chức trước các rủi ro pháp lý và nâng cao tính an toàn thông tin cho hệ thống.