

MỤC TIÊU CỦA CHƯƠNG 14:

- **Hiểu nền tảng cho các vấn đề pháp lý và đạo đức trong EC.**
- **Mô tả luật sở hữu trí tuệ và hiểu về xét xử.**
- **Giải thích các vấn đề về quyền riêng tư và tự do ngôn luận cũng như những thách thức của chúng.**
- **Mô tả các loại gian lận trên Internet và cách bảo vệ**
- **chống lại chúng.**
- **Mô tả các nhu cầu và phương pháp để bảo vệ cả người mua và**
- **người bán.**
- **Mô tả các vấn đề xã hội liên quan đến EC.**
- **Mô tả Green EC và IT.**

1. Các thách thức về đạo đức

Các tiêu chuẩn đạo đức dành cho các cá nhân/ tổ chức:

- Tôn trọng tự chủ
- Không gây hại
- Công bằng
- Trung thực và minh bạch
- Bảo mật thông tin
- Chuyên nghiệp: hành xử chuyên nghiệp và tuân thủ các tiêu chuẩn và quy tắc đạo đức chuyên nghiệp.
- Trách nhiệm xã hội doanh nghiệp: Nghĩa vụ của các doanh nghiệp đóng góp vào sự phát triển bền vững, bao gồm bảo vệ quyền con người, môi trường và lợi ích của các bên liên quan.
- Tránh xung đột lợi ích
- Tuân thủ pháp luật và các quy định áp dụng

Các vấn đề đạo đức trong TMĐT

- Quyền riêng tư và bảo vệ dữ liệu: Các trang web thương mại điện tử thu thập lượng lớn thông tin cá nhân về khách hàng, bao gồm tên, địa chỉ, số điện thoại và thông tin thẻ tín dụng. Thông tin này có giá trị đối với các tội phạm mạng và có thể được sử dụng cho việc trộm danh hay các hoạt động gian lận khác.
- An ninh mạng: Với sự phát triển ngày càng phụ thuộc vào thương mại điện tử, các mối đe dọa mạng trở thành một vấn đề lớn đối với các doanh nghiệp và người tiêu dùng. Các giao dịch trực tuyến dễ bị tấn công bởi các phương

thức tấn công mạng, lừa đảo và các loại tấn công mạng khác có thể đe dọa đến thông tin cá nhân và tài chính.

- Sở hữu trí tuệ: Các trang web thương mại điện tử làm cho việc sao chép, phân phối và bán tài liệu được bảo vệ bản quyền một cách dễ dàng mà không có sự cho phép từ chủ sở hữu. Điều này đã dẫn đến sự gia tăng về việc vi phạm bản quyền và đạo văn trực tuyến, có thể gây hại đến các ngành sáng tạo và giảm sự khuyến khích để tạo ra nội dung mới.
- Cạnh tranh công bằng: Thương mại điện tử đã làm cho việc cạnh tranh trở nên dễ dàng hơn cho các doanh nghiệp toàn cầu, nhưng cũng đã dẫn đến các hành vi phi đạo đức như là thỏa thuận giá, cộng tác và hành vi thống trị thị trường. Điều này có thể gây hại cho các doanh nghiệp nhỏ và hạn chế sự lựa chọn của người tiêu dùng.
- Thực tiễn lao động: Các công ty thương mại điện tử phụ thuộc rất nhiều vào dịch vụ hậu cần và giao hàng, thường được cung cấp bởi các nhà thầu bên thứ ba. Các nhà thầu này có thể không nhận được mức lương hoặc lợi ích công bằng, dẫn đến bóc lột lao động và điều kiện làm việc không công bằng.
- Tác động môi trường: Sự phát triển của thương mại điện tử đã dẫn đến sự gia tăng của chất thải đóng gói và lượng khí thải carbon từ vận chuyển. Điều này có thể gây hại cho môi trường và đóng góp vào thay đổi khí hậu.

2. Luật sở hữu trí tuệ

Sở hữu trí tuệ trong TMDT

Sở hữu trí tuệ là một khía cạnh quan trọng của thương mại điện tử. Nó đề cập đến các tài sản vô hình như thương hiệu, sáng chế, bản quyền và bí mật thương mại. Các nền tảng thương mại điện tử và các thị trường trực tuyến cho phép các doanh nghiệp phân phối sản phẩm và dịch vụ của họ trên toàn cầu, điều này có thể tăng giá trị của các tài sản sở hữu trí tuệ của họ. Tuy nhiên, điều này cũng làm cho họ dễ bị vi phạm hơn.

Trong thương mại điện tử, có một số vấn đề về sở hữu trí tuệ mà các doanh nghiệp cần phải nhận thức, bao gồm:

- Vi phạm thương hiệu: Các nền tảng thương mại điện tử thường được sử dụng bởi những kẻ làm giả để bán hàng giả hoặc hàng đạo nhái vi phạm thương hiệu của một công ty. Điều này có thể làm hại đến danh tiếng của công ty và gây thiệt hại tài chính.

- Vi phạm bản quyền: Các nền tảng thương mại điện tử cũng có thể được sử dụng để bán các bản sao bất hợp pháp hoặc không có quyền của các tác giả được bảo vệ bản quyền, chẳng hạn như sách, âm nhạc và phim. Điều này có thể dẫn đến thiệt hại tài chính đáng kể cho các tác giả của những tác phẩm này.
- Vi phạm sáng chế: Các nền tảng thương mại điện tử cũng có thể được sử dụng để bán các sản phẩm vi phạm công nghệ được bảo hộ bởi sáng chế của một công ty, dẫn đến thiệt hại tài chính đáng kể và có thể phải đưa ra hành động pháp lý.
- Vi phạm bí mật thương mại: Các nền tảng thương mại điện tử cũng có thể được sử dụng để bán các sản phẩm sử dụng bí mật thương mại của một công ty mà không được sự cho phép của họ, chẳng hạn như các công thức hay quy trình bí mật.

Để bảo vệ tài sản sở hữu trí tuệ của mình, các doanh nghiệp nên thực hiện các biện pháp tích cực như:

- Đăng ký thương hiệu, bản quyền và sáng chế của họ: Điều này giúp đảm bảo rằng tài sản sở hữu trí tuệ của họ được bảo vệ bởi luật pháp và có thể sử dụng để đưa ra hành động pháp lý khi cần thiết.
- Theo dõi các nền tảng thương mại điện tử và các thị trường trực tuyến để phát hiện các sản phẩm vi phạm sở hữu trí tuệ: Các doanh nghiệp có thể sử dụng các công cụ để theo dõi các sản phẩm được bán trên các nền tảng và thị trường này và đưa ra hành động pháp lý khi cần thiết.
- Xây dựng chiến lược bảo vệ sở hữu trí tuệ: Các doanh nghiệp nên xem xét xây dựng một chiến lược bảo vệ sở hữu trí tuệ toàn diện, bao gồm cả bảo vệ tài sản sở hữu trí tuệ của họ và theo dõi các sản phẩm vi phạm sở hữu trí tuệ của đối thủ cạnh tranh.
- Tăng cường giám sát và quản lý nhân viên và đối tác: Để ngăn chặn việc rò rỉ bí mật thương mại hoặc việc sử dụng tài sản sở hữu trí tuệ của công ty một cách trái phép, các doanh nghiệp cần tăng cường giám sát và quản lý nhân viên và đối tác.
- Đưa ra hành động pháp lý khi cần thiết: Khi phát hiện các vi phạm sở hữu trí tuệ, các doanh nghiệp cần đưa ra hành động pháp lý để bảo vệ tài sản sở hữu trí tuệ của họ và ngăn chặn các vi phạm tương lai.

3. Quyền riêng tư, bảo vệ và tự do ngôn luận

Quyền riêng tư và tự do ngôn luận đều là quyền cơ bản và được đảm bảo trong nhiều quy định pháp luật ở nhiều quốc gia trên thế giới. Trong lĩnh vực thương mại điện tử, hai

quyền này đóng vai trò quan trọng và cần phải được cân nhắc để đảm bảo một môi trường kinh doanh trực tuyến lành mạnh và công bằng.

Quyền riêng tư trong thương mại điện tử

Quyền riêng tư trong thương mại điện tử liên quan đến việc bảo vệ thông tin cá nhân của khách hàng trực tuyến. Các doanh nghiệp thương mại điện tử phải tuân thủ các quy định về bảo vệ dữ liệu cá nhân của khách hàng, bao gồm việc thu thập, sử dụng và bảo mật thông tin cá nhân. Các quy định này có thể bao gồm việc yêu cầu sự đồng ý của khách hàng trước khi thu thập thông tin, giới hạn việc sử dụng thông tin chỉ để mục đích nhất định và phải bảo mật thông tin đó.

Tự do ngôn luận trong thương mại điện tử:

Tự do ngôn luận trong thương mại điện tử là quyền của các doanh nghiệp và cá nhân được tự do phát biểu ý kiến, tạo ra nội dung và chia sẻ thông tin trên mạng. Tuy nhiên, tự do ngôn luận cũng phải tuân thủ các quy định pháp luật, bao gồm các quy định về bản quyền, quyền riêng tư và các quy định về vi phạm an ninh mạng.

- ⇒ Để đảm bảo sự cân bằng giữa quyền riêng tư và tự do ngôn luận, các quy định và chính sách phù hợp cần được đưa ra và các doanh nghiệp thương mại điện tử cần phải tuân thủ những quy định này. Ngoài ra, việc tăng cường giáo dục và nâng cao nhận thức của người dùng cũng là một phần quan trọng để đảm bảo sự an toàn và bảo mật trong thương mại điện tử.

Cách thông tin về cá nhân được thu thập và sử dụng trực tuyến

- Mẫu đăng ký trực tuyến: Khi khách hàng đăng ký tài khoản hoặc đăng ký nhận thông tin từ trang web, họ sẽ được yêu cầu điền vào một mẫu đăng ký trực tuyến. Thông tin cá nhân của khách hàng, chẳng hạn như tên, địa chỉ email, địa chỉ nhà, số điện thoại và ngày sinh, có thể được thu thập thông qua mẫu đăng ký này.
- Hình thức thanh toán trực tuyến: Khi khách hàng thanh toán cho sản phẩm hoặc dịch vụ trên trang web, thông tin về thẻ tín dụng của họ sẽ được yêu cầu. Thông tin này có thể bao gồm số thẻ tín dụng, ngày hết hạn, mã bảo mật và tên chủ thẻ.
- Cookie: Cookie là các tệp văn bản nhỏ được lưu trữ trên máy tính của người dùng khi họ truy cập trang web. Các cookie này có thể thu thập thông tin về các hoạt động của người dùng trên trang web, chẳng hạn như các trang web đã xem, quảng cáo đã nhấp vào, v.v.
- Địa chỉ IP: Địa chỉ IP là địa chỉ duy nhất được cấp phát cho mỗi thiết bị khi truy cập internet. Các trang web có thể thu thập địa chỉ IP của người dùng để phân tích hoạt động trên trang web hoặc để cung cấp dịch vụ định vị.

Bảo vệ tự riêng tư bằng công nghệ thông tin

- Mã hóa: Các trang web có thể sử dụng mã hóa để bảo vệ thông tin cá nhân của khách hàng khi chúng được truyền qua mạng. Mã hóa là quá trình mã hóa thông tin sao cho chỉ người nhận có thể giải mã nó. Việc sử dụng mã hóa giúp đảm bảo rằng thông tin cá nhân của khách hàng không bị đánh cắp hoặc lộ ra cho bên thứ ba.
- Chứng chỉ SSL: Chứng chỉ SSL (Secure Socket Layer) là một cơ chế bảo mật được sử dụng để xác thực trang web và bảo vệ thông tin được truyền qua mạng. Các trang web có chứng chỉ SSL được mã hóa và đảm bảo rằng thông tin cá nhân của khách hàng được bảo vệ trong quá trình truyền tải.
- Hệ thống chống virus và phần mềm gián điệp: Các trang web có thể sử dụng các hệ thống chống virus và phần mềm gián điệp để bảo vệ khách hàng khỏi các mối đe dọa mạng trực tuyến. Điều này giúp đảm bảo rằng thông tin cá nhân của khách hàng không bị đánh cắp hoặc lộ ra cho bên thứ ba.
- Quy định về quyền riêng tư: Các trang web có thể áp dụng các quy định về quyền riêng tư và chính sách bảo mật để bảo vệ thông tin cá nhân của khách hàng. Điều này giúp đảm bảo rằng khách hàng được cung cấp thông tin về cách thông tin của họ được sử dụng và chia sẻ.

Vấn đề riêng tư trong công cụ web 2.0 và mạng xã hội

- Thu thập thông tin cá nhân: Các mạng xã hội có thể thu thập thông tin cá nhân của người dùng, chẳng hạn như tên, địa chỉ, số điện thoại, email và thông tin về sở thích. Những thông tin này có thể được sử dụng để tạo ra quảng cáo đích danh hoặc bán cho bên thứ ba để sử dụng vào mục đích quảng cáo.
- Quảng cáo đích danh: Các mạng xã hội có thể sử dụng thông tin cá nhân để tạo ra quảng cáo đích danh cho người dùng. Quảng cáo đích danh là những quảng cáo được tùy chỉnh cho từng người dùng dựa trên các thông tin cá nhân của họ.
- Phân tích hành vi người dùng: Các mạng xã hội có thể phân tích hành vi người dùng để hiểu rõ hơn về sở thích và thói quen của họ. Những thông tin này có thể được sử dụng để tùy chỉnh nội dung và quảng cáo đến người dùng.
- Nguy cơ mất quyền riêng tư: Nhiều người dùng không nhận ra rằng các thông tin cá nhân của họ đang được thu thập và chia sẻ trên mạng xã hội. Họ có thể chia sẻ những thông tin riêng tư với bạn bè hoặc nhóm mà không nhận ra rằng thông tin đó có thể được chia sẻ rộng rãi trên mạng.

Bảo vệ riêng tư theo các nguyên tắc đạo đức

- Nguyên tắc minh bạch: Các tổ chức cần phải thông báo rõ ràng cho người dùng về việc thu thập, sử dụng và chia sẻ thông tin cá nhân của họ, và phải cho phép người dùng kiểm soát thông tin của mình.
- Nguyên tắc chấp nhận: Các tổ chức cần phải chấp nhận trách nhiệm của mình trong việc bảo vệ thông tin cá nhân của người dùng, và phải tuân thủ các quy định và luật pháp liên quan đến quyền riêng tư.
- Nguyên tắc độc lập: Các tổ chức cần phải đảm bảo độc lập của mình trong việc thu thập, sử dụng và chia sẻ thông tin cá nhân của người dùng, và không được ảnh hưởng bởi các bên thứ ba.
- Nguyên tắc trách nhiệm: Các tổ chức cần phải chịu trách nhiệm đối với việc bảo vệ thông tin cá nhân của người dùng, và phải có các chính sách và quy trình để xử lý việc vi phạm bảo vệ quyền riêng tư của người dùng.
- Nguyên tắc đồng thuận: Các tổ chức cần phải thu được sự đồng thuận của người dùng trước khi thu thập, sử dụng hoặc chia sẻ thông tin cá nhân của họ.

4. Các vấn đề pháp lý khác của TMDT

Môi trường pháp lý và quy định

Ở Việt Nam, có một số đạo luật pháp lý liên quan đến bảo vệ quyền riêng tư trên mạng như sau:

Luật An ninh mạng số 24/2018/QH14: Luật này quy định về việc bảo vệ an ninh mạng và chống lại các hành vi vi phạm an ninh mạng, bao gồm các hành vi xâm nhập, tấn công, làm gián đoạn hoặc xóa mất dữ liệu.

Luật Quảng cáo số 16/2012/QH13: Luật này quy định về quảng cáo trên mạng, yêu cầu các tổ chức và cá nhân có trách nhiệm bảo vệ quyền lợi và sở hữu trí tuệ của người tiêu dùng.

Luật Quy hoạch, sửa đổi, bổ sung một số điều của Luật Công nghệ thông tin số 67/2006/QH11: Quy định về việc bảo vệ thông tin cá nhân, nghĩa vụ của các tổ chức và cá nhân thu thập, sử dụng và chia sẻ thông tin cá nhân của người dùng.

Bắt nạt trực tuyến

Cyberbullying (hay còn gọi là bắt nạt trực tuyến) là hành vi sử dụng các công nghệ truyền thông điện tử như mạng xã hội, tin nhắn văn bản hoặc email để quấy rối, đe dọa hoặc gây thiệt hại cho người khác. Nó có thể có nhiều hình thức khác nhau, bao gồm tung tin đồn hoặc lời nói dối, đe dọa, gửi tin nhắn hoặc hình ảnh độc hại, và loại bỏ ai đó khỏi các nhóm hoặc hoạt động trực tuyến.

Cyberbullying có thể gây những hậu quả nghiêm trọng cho nạn nhân, bao gồm trầm cảm, lo âu và thậm chí là tự tử. Đó cũng là một vấn đề ngày càng được quan tâm tại các trường học và nơi làm việc, nơi nó có thể ảnh hưởng tiêu cực đến môi trường học tập và làm việc.

Đề đối phó với cyberbullying, tại Việt Nam đã cho ban hành một số đạo luật, quy định đối với các mạng xã hội tuy nhiên vẫn còn nhiều hạn chế.

Ngoài các biện pháp pháp lý, cũng có nhiều chương trình giáo dục và tài nguyên có sẵn để giúp ngăn chặn cyberbullying và hỗ trợ nạn nhân. Điều này bao gồm các mẹo an toàn trực tuyến, dịch vụ tư vấn và các chiến dịch chống bắt nạt tại các trường học và cộng đồng.

5. Bảo vệ người tiêu dùng và người bán khỏi gian lận trực tuyến

Bảo vệ người tiêu dùng

- Sử dụng các trang web an toàn: Tìm kiếm các trang web có chứng chỉ SSL hoặc biểu tượng khóa ở thanh địa chỉ trình duyệt.
- Bảo vệ thông tin cá nhân: Không bao giờ cung cấp thông tin nhạy cảm cho bất kỳ ai trực tuyến trừ khi đó là một trang web đáng tin cậy.
- Sử dụng mật khẩu mạnh
- Cảnh trọng với các trò lừa đảo phishing: Cảnh trọng với các email hoặc tin nhắn yêu cầu thông tin cá nhân hoặc yêu cầu nhấp vào một liên kết. Những cái này có thể là các trò lừa đảo phishing được thiết kế để đánh cắp thông tin.
- Sử dụng nhà cung cấp đáng tin cậy
- Kiểm tra tài khoản của bạn thường xuyên
- Sử dụng phần mềm chống virus và bảo mật
- Báo cáo gian lận

Bảo vệ người bán

- Sử dụng phương thức thanh toán an toàn
- Xác minh thông tin của người mua: Trước khi gửi hàng, xác minh thông tin của người mua, chẳng hạn như địa chỉ vận chuyển và thông tin liên lạc của họ. Đảm bảo thông tin phù hợp với thông tin thanh toán để đảm bảo rằng bạn đang giao dịch với một người mua hợp pháp.
- Sử dụng theo dõi và xác nhận giao hàng: Sử dụng phương thức vận chuyển bao gồm theo dõi và xác nhận giao hàng. Điều này sẽ cung cấp bằng chứng rằng hàng đã được giao cho người mua.

- Liên lạc với người mua: Duy trì liên lạc mở với người mua trong suốt giao dịch. Trả lời nhanh chóng các câu hỏi và quan tâm của họ. Điều này sẽ giúp xây dựng niềm tin và ngăn ngừa sự hiểu nhầm.
- Cảnh trọng với hành vi đáng ngờ: Hãy cảnh trọng với bất kỳ hành vi đáng ngờ nào, chẳng hạn như người mua yêu cầu hoàn tiền trước khi hàng được nhận hoặc yêu cầu địa chỉ vận chuyển khác với địa chỉ được liệt kê trên thông tin thanh toán. Hãy tin vào trực giác của bạn và thực hiện các biện pháp phòng ngừa nếu có điều gì đó không đúng.

Chữ ký điện tử và chữ ký số

Chữ ký điện tử và chữ ký số được sử dụng để bảo vệ cả người mua và người bán trong các giao dịch trực tuyến. Ví dụ, chữ ký điện tử có thể được sử dụng để ký hợp đồng bán hàng hoặc dịch vụ, trong khi chữ ký số có thể được sử dụng để xác nhận tính xác thực của hợp đồng và danh tính của người ký. Điều này giúp ngăn ngừa gian lận và đảm bảo rằng cả hai bên đều được bảo vệ.

6. Các vấn đề xã hội và TMDT xanh

Cách biệt số hoá (digital divide)

Là khoảng cách giữa những người có quyền truy cập vào các công nghệ kỹ thuật số, như internet, máy tính và điện thoại thông minh và những người không có.

Ở mức cá nhân, cách biệt số hoá có thể dẫn đến sự bất đồng về quyền truy cập vào giáo dục, cơ hội việc làm và sự tham gia xã hội và chính trị. Những người thiếu quyền truy cập vào các công nghệ kỹ thuật số có thể bỏ lỡ cơ hội để học hỏi và phát triển kỹ năng, điều này có thể hạn chế khả năng tham gia đầy đủ vào nền kinh tế và xã hội.

Ở mức cộng đồng, cách biệt số hoá có thể dẫn đến sự bất đồng về quyền truy cập vào thông tin và tài nguyên, điều này có thể hạn chế khả năng của các cộng đồng giải quyết các vấn đề kinh tế và xã hội. Các cộng đồng không có quyền truy cập vào các công nghệ kỹ thuật số có thể gặp khó khăn trong việc truy cập thông tin chăm sóc sức khỏe, cơ hội việc làm và các tài nguyên khác có thể cải thiện chất lượng cuộc sống của họ. Điều này có thể góp phần tạo ra một chuỗi nghèo đói và cô lập khó khăn để đập tan.

Ở mức toàn cầu, cách biệt số hoá thể hiện khoảng cách giữa các nước phát triển và đang phát triển về quyền truy cập vào các công nghệ kỹ thuật số. Những nước đang phát triển có thể thiếu hạ tầng, tài nguyên và chính sách cần thiết để hỗ trợ việc áp dụng rộng rãi

các công nghệ kỹ thuật số, điều này có thể hạn chế khả năng của họ tham gia đầy đủ vào nền kinh tế và xã h

Để giải quyết vấn đề chia sẻ kỹ thuật số, cần có các nỗ lực tập trung vào việc đưa các công nghệ kỹ thuật số vào tầm với của tất cả mọi người. Các giải pháp có thể bao gồm tăng cường quyền truy cập internet, giảm chi phí đăng ký thiết bị kỹ thuật số và tăng cường khả năng kỹ thuật số cho các cộng đồng và quốc gia đang phát triển.

Làm việc từ xa (Telecommuting)

Là một hình thức làm việc mà nhân viên có thể làm việc từ một địa điểm khác với văn phòng của nhà tuyển dụng. Điều này có thể được thực hiện thông qua việc sử dụng công nghệ như máy tính, truy cập internet và hội nghị truyền hình.

Telecommuting đã trở nên ngày càng phổ biến trong những năm gần đây, khi các tiến bộ về công nghệ đã làm cho việc làm việc từ xa trở nên dễ dàng hơn. Tuy nhiên, telecommuting cũng có thể gặp phải những thách thức, chẳng hạn như thiếu tương tác xã hội và sự mất tập trung khi làm việc tại nhà. Quan trọng là nhà tuyển dụng phải thiết lập các quy định và mong đợi rõ ràng cho nhân viên làm việc từ xa, và cho nhân viên duy trì một môi trường làm việc chuyên nghiệp ngay cả khi làm việc tại nhà.

Green computing (điện toán xanh)

Green computing, hay green IT, đề cập đến việc thiết kế, phát triển, sử dụng và xử lý các máy tính, máy chủ và các hệ thống phụ trợ đi kèm một cách bền vững với môi trường. Mục tiêu của green computing là giảm ảnh hưởng của công nghệ tính toán đến môi trường bằng cách giảm tiêu thụ năng lượng, giảm rác điện tử và khuyến khích sử dụng các nguồn tài nguyên tái tạo.

Green computing là một khía cạnh quan trọng của bền vững trong thế giới hiện đại, khi việc sử dụng công nghệ tính toán tiếp tục tăng lên và tiêu thụ năng lượng và tài nguyên. Bằng cách khuyến khích hiệu quả năng lượng và các phương pháp xử lý đúng cách, và khai thác các nguồn tài nguyên tái tạo, green computing có thể giúp giảm ảnh hưởng của công nghệ tính toán đến môi trường và đóng góp vào một tương lai bền vững hơn